



Calhoun: The NPS Institutional Archive
DSpace Repository

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

2008-09

Integration and interoperability an analysis to identify the attributes for system of systems

Turso, Denise L.

Monterey, California. Naval Postgraduate School

<http://hdl.handle.net/10945/3907>

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**INTEGRATION AND INTEROPERABILITY: AN ANALYSIS TO
IDENTIFY THE ATTRIBUTES FOR SYSTEM OF SYSTEMS**

by

John E. Gay
Denise L. Turso

September 2008

Thesis Advisor:
Second Readers:

John Osmundson
Scott Bey
Henry Cook

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE September 2008	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Integration and Interoperability: An Analysis to Identify the Attributes for System of Systems			5. FUNDING NUMBERS	
6. AUTHOR(S) John E. Gay, Denise L. Turso				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) A system of systems design is the development of multiple systems that individually provide various functions that collectively support a holistic functional capability. With the evolution of today's increased demand of heterogeneous systems that integrate to form complex system of systems, integration and interoperability are critical to cost, schedule and performance during the lifecycle of a product. Enterprises must explore and discover the current and future techniques of building both human and technical systems that requires a deep knowledge and understanding of integration and interoperability. In support of this goal, this thesis, through research and analysis, develops a descriptive and prescriptive approach to assist management in achieving integration and interoperability. This thesis discovers the key attributes that result in an integrated and interoperable system and determines new procedures and techniques that can be recommended to achieve the system engineering required to support interoperability and ensure integration of system of systems.				
14. SUBJECT TERMS System of Systems, Family of Systems, Enterprise, Integration, Interoperability, Framework, Statutory Laws, Regulatory Laws, Descriptive Model, Normative Model, Prescriptive Model, C4ISR, I2 Analysis, Learning Management System, Enterprise Resource Planning (ERP)			15. NUMBER OF PAGES 115	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**INTEGRATION AND INTEROPERABILITY: AN ANALYSIS TO IDENTIFY
THE ATTRIBUTES FOR SYSTEM OF SYSTEMS**

John E. Gay

Director, Marine Air Ground Task Force (MAGTF) & Joint Integration and Certification
(M&JIC) Division, United States Marine Corps Systems Command, Quantico, Virginia
B.S., University of South Florida, 1988

Denise L. Turso

Systems Engineer, Northrop Grumman Shipbuilding
B. S., The Pennsylvania State University, 1989
M.Ed., The Pennsylvania State University, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
September 2008**

Author: John E. Gay

Denise L. Turso

Approved by: John Osmundson
Thesis Advisor

Scott Bey
Second Reader

Henry Cook
Second Reader

David H. Olwell
Chairman, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

A system of systems design is the development of multiple systems that individually provide various functions that collectively support a holistic functional capability. With the evolution of today's increased demand for heterogeneous systems that integrate to form complex system of systems, integration and interoperability are critical to cost, schedule, and performance during the lifecycle of a product. Successful integration and interoperability must be achieved for future system of systems. Enterprises must explore and discover the current and future techniques of building both human and technical systems that requires a deep knowledge and understanding of integration and interoperability. In support of this goal, this thesis, through research and analysis, develops a descriptive and prescriptive approach to assist management in achieving integration and interoperability. This thesis discovers the key attributes that result in an integrated and interoperable system and determines new procedures and techniques that can be recommended to achieve the system engineering required to support interoperability and ensure integration of system of systems.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	BACKGROUND	1
B.	PURPOSE.....	2
C.	RESEARCH QUESTIONS.....	2
D.	BENEFITS OF STUDY.....	2
E.	SCOPE AND METHODOLOGY	3
II.	CROSSWALK OF C4I I2 DOCUMENTED “RULES”	5
A.	INTRODUCTION.....	5
B.	BEHIND THE LAWS.....	5
C.	STATUTORY LAWS.....	6
D.	REGULATORY LAWS	7
E.	SUMMARY	7
III.	RESEARCH OF SUCCESSFUL INTEGRATION AND INTEROPERABILITY OF SYSTEM OF SYSTEMS DESIGNS	9
A.	INTRODUCTION.....	9
B.	BACKGROUND	13
C.	CRITERIA USED FOR SELECTION OF PROGRAMS	15
D.	OVERVIEW OF PROGRAMS	16
1.	NASA Space Shuttle and Apollo Program	16
2.	Future Combat System Program	18
3.	Rail Controls.....	21
4.	DoD Joint Distributed Common Ground Systems Program	23
5.	Learning Management System	27
E.	SUMMARY	28
IV.	RESEARCH OF UNSUCCESSFUL INTEGRATION AND INTEROPERABILITY OF SYSTEM OF SYSTEMS DESIGNS	31
A.	INTRODUCTION.....	31
B.	OVERVIEW OF PROGRAMS	31
1.	Combat ID	31
2.	Coast Guard Deepwater Program.....	34
3.	Unmanned Air Vehicles.....	37
4.	Enterprise Joint System	40
C.	SUMMARY	43
V.	SYSTEM OF SYSTEMS INTEGRATION AND INTEROPERABILITY FRAMEWORK.....	47
A.	INTRODUCTION.....	47
B.	SYSTEM OF SYSTEMS I² FRAMEWORK	48
1.	Standardized Attributes for Models.....	50
2.	Normative Model (Notional)	51

C.	GAP ANALYSIS USING SYSTEM OF SYSTEMS FRAMEWORK FOR I2.....	52
1.	Unmanned Air Vehicles Analysis	52
a.	<i>Unmanned Air Vehicles Descriptive and Normative Model.....</i>	52
b.	<i>Unmanned Air Vehicles Prescriptive Model.....</i>	53
2.	Future Combat System Analysis	54
a.	<i>Future Combat System Descriptive and Normative Model...54</i>	
3.	Enterprise Joint System Analysis	55
a.	<i>Enterprise Joint System Descriptive and Normative Model..55</i>	
b.	<i>Enterprise Joint System Prescriptive Model</i>	56
D.	SUMMARY	57
1.	I ² Analysis	57
VI.	CONCLUSION	61
A.	KEY RESEARCH FINDINGS	61
B.	LESSONS LEARNED	61
1.	How do the Current Policies and Processes of Successful Large System of Systems Designs Support I ² ?	61
2.	How Effective are the Existing Laws and DoD Instructions in ensuring Integration and Interoperability?	62
3.	What are the Key Attributes that Result in an I2 System?.....	63
a.	<i>Common and Known Operational Environment.....</i>	63
b.	<i>Governance of the I2 Boundaries</i>	64
c.	<i>I² Based Acquisition, Not Schedule or Funding.....</i>	65
d.	<i>Early Establishment of I² Requirements.....</i>	65
4.	What New Recommendations Can Support Interoperability and Ensure Integration of System of Systems?	66
a.	<i>Improve Capability Architecting</i>	66
b.	<i>Modeling and Simulation</i>	66
c.	<i>Operational Assessments during Development Test.....</i>	67
C.	FUTURE RESEARCH.....	67
APPENDIX A.	STATUTORY LAWS	69
A.	PUBLIC LAW 104-106-FEB. 10, 1996	69
B.	PUBLIC LAW 105-261-OCT. 17, 1998.....	71
C.	PUBLIC LAW 107-314-DEC. 2, 2002.....	74
APPENDIX B.	REGULATORY LAWS.....	79
A.	JOINT PUBLICATION 1	79
B.	JOINT PUBLICATION 6	81
C.	CHAIRMAN OF THE JOINT CHIEF OF STAFF INSTRUCTIONS	86
1.	CJCSI 3100.01A September 1, 1999, Directive Current as of September 12, 2003	86
2.	CJCSI 6212.01D March 8, 2006, Directive Current as of March 14, 2007.....	86

D. DOD INSTRUCTION 4630.8, PROCEDURE FOR INTEROPERABILITY AND SUPPORTABILITY OF INFORMATION TECHNOLOGY (IT) AND NATIONAL SECURITY SYSTEMS (NSS)	87
LIST OF REFERENCES.....	89
INITIAL DISTRIBUTION LIST	95

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	System of Systems – Emergent Behaviors	12
Figure 2.	Douglas Archibald Surveillance Kite 1883	37
Figure 3.	V-1 designed by Fieseler and Argus Motoren	38
Figure 4.	History of IT Integration	40
Figure 5.	History of IT Integration	42
Figure 6.	I ² Analysis Stages.	58

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	A Simple Typology of Technological Systems	9
Table 2.	Advantages of Standard Interfaces	11
Table 3.	A Simple Typology of Technological Systems with Nine System of Systems	48
Table 4.	System of Systems I ² Framework	49
Table 5.	Definitions and Standardized Attributes for Descriptive Table.....	51
Table 6.	Standardized Attributes for Normative Notional Model	52
Table 7.	Unmanned Air Vehicles Description and Normative Model.....	53
Table 8.	Unmanned Air Vehicles Prescriptive Model	54
Table 9.	Future Combat System Descriptive and Normative Model.....	55
Table 10.	Enterprise Joint System Descriptive and Normative Model.....	56
Table 11.	Enterprise Joint System Prescriptive Model	57

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENT

The authors are grateful for the support of this work by Assistant Secretary Navy, Research Development Acquisition (ASN RDA), United States Marine Corps, and Northrop Grumman Ship Building-Gulf Coast. Being given this opportunity to earn a Masters of Science in System Engineering Management from the Naval Postgraduate School is sincerely appreciated and would not have been possible without the support of our organization managers, a number of first-rate professors, and our family and friends.

Without the financial support and commitment by Assistant Secretary Navy, Research Development Acquisition (ASN RDA) Chief Systems Engineering, Mr. Carl Siel related to the PD 21 Systems Engineering Program, our participation would not have been possible.

The most important thanks the authors could offer goes to our families.

To John's wife and kids: Yvonne, your love, encouragement, and patience enabled the completion of this work. You have been a friend and supporting wife and have done an incredible job raising and parenting our kids without much involvement by me over the past two years. To my kids, Meagan and Connor, you are my joy and inspiration and I love you both more than you will ever know. Semper Fi

To Denise's husband Jim - my friend and partner in life, thank you for your positive attitude and vision throughout the past two years. Your consistent encouragement and patience has enabled the completion of this degree. I am most grateful and appreciative.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

With the evolution of today's increasing demand for heterogeneous systems that integrate to form complex system of systems, integration and interoperability are critical to cost, schedule and performance during the lifecycle of a product. The development of commercial and military capabilities that depend on a system of systems design using Command and Control, Computer, Communication, and Intelligence Systems (C4I) or net-centric based design needs to be both integrated and interoperable to ensure effective capabilities are fielded.

Some within the acquisition community believe the statutory laws, regulatory laws, and various Department of Defense instructions related to program acquisition are all that is required for developing integrated and interoperable solutions. This thesis examines a sample of the eighty eight laws and instructions found that reference either integration or interoperability. Given the lack of scope and definition used in these documents, it is unlikely they will ensure system of systems is integrated and interoperable.

The goal of this thesis, through research, analysis, and synthesis was to review successful and unsuccessful programs and build a foundation to understand system design characteristics. A modeling approach was used to discover key attributes that resulted in an integrated and interoperable system and provide identification of procedures and techniques that can be recommended to program managers to achieve the system engineering required to support interoperability and ensure integration of system of systems. The procedures and techniques recommended for any future integration and interoperability are in the areas of 1) capability architecting, 2) modeling and simulation, and 3) operational assessment during development testing.

The research, investigation, and analysis of system integration and interoperability conducted as part of this thesis establishes a pro-active approach to successful integration and interoperability system designs and a framework that could be used to evaluate, normalize and prescribe corrections within a lifecycle of a program.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The development and fielding of system of systems continues to result in non-integrated and non-interoperable systems that deliver less than expected capabilities. For system of systems programs, “**integration** and **interoperability** (I^2)” is critical to success. The meaning of these words will guide the discussion of this thesis (Agnes, 2006).

integrate: to make whole or complete by adding or bringing together parts; unify.

interoperability: the ability of a system or component to function effectively with other systems or components.

Systems integration is not simply an engineering or operations task, it encompasses technical, strategic and organizational capabilities (Hobday, Davies, & Prencipe, 2005). The systems integration process provides assurance to the customer that all system elements will function as a whole. Systems integration extends to the holistic notion that involves all of the organizational components of an enterprise during the entire cycle of the acquisition process. Interoperability solutions for an acquisition require comprehensive integration strategies that go beyond simple connections. Largely, successful integration depends on maintaining a system perspective (Rifley, 2008).

The introduction of net-centric warfare, an architectural foundation that integrates all Department of Defense (DoD) information systems, requires interoperability across an increasing number of C4I systems to work together harmoniously to deliver a warfighting capability. The integration and interoperability of an infrastructure is paramount, because the advantage of net-centric warfare is sharing information through people, processes, and technology. This thesis will determine if the current laws, DoD instructions, systems engineering steps within a program acquisition, and/or culture within an enterprise are inhibiting or improving the integration of system of systems.

B. PURPOSE

This research explores the cause(s) of DoD system of systems non-integration and non-interoperability and the challenges that are involved. This research will identify the key components to “integration and interoperability (I²)” required for systems designs and identify potential roadblocks of fielding effective I² systems.

C. RESEARCH QUESTIONS

The implementation of the various policies and processes regarding I² systems that impact a system’s design do not always have the expected outcome. In some cases, the cause(s) of system of systems non-integration and non-interoperability are related to other attributes not defined in these policies and processes. The following questions were designed to understand the challenges and opportunities to identify not only an interoperable system (all parts work together to form a whole) but an integrated system (all parts interact seamlessly, in a synchronized fashion).

1. How do the current policies and processes of successful large system of systems designs support I²?
2. How effective are the existing laws and DoD instructions in ensuring integration and interoperability?
3. What are the key attributes that result in an integrated and interoperable system?
4. What new procedures or techniques can be recommended to determine the system engineering required to support interoperability and ensure integration of system of systems?

D. BENEFITS OF STUDY

System of systems being developed or currently fielded are not taking into account integration beyond the immediate system interface boundary, through legacy requirements or misuse of capability based requirements. New approaches need to be explored to address the challenges of the large scale, rapid pace, and simultaneous efforts of system of systems development (Kaplan, 2006).

The requirement to use standard interfaces have improved point-to-point interoperability but have not consistently improved the integration of multiple system of systems. Many advocates propose the use of “standards” for these types of interfaces. The interface standards are not always written clearly; thereby, allowing “interpretation” of these standards. The resolution of these loopholes within the interface standards have been slow to resolve and slower to implement.

The warfighter is faced with the challenge of making systems with individual capabilities interoperate within the current system of systems environment, as new individual systems are fielded. The requirement for integrated and interoperable system of systems is essential to enable a net-centric environment.

This analytical review seeks to look past the symptoms of systems that lack I^2 and look at the criticality of non-integration and non-interoperability. Research into the current policies, processes, examples of successful I^2 systems design, and examples of challenged I^2 systems design will determine the gaps and opportunities for better I^2 . This thesis will recommend ways to identify and improve designs with concern to I^2 for future systems.

E. SCOPE AND METHODOLOGY

This thesis will focus on systems within a larger system of systems environment. The research and analysis will be related to the cause of non-integration and non-interoperability in current acquisitions and equipment fielding. Competitive advantage in business and war requires capabilities that result from the interoperability of systems and the integration of many processes (Kaplan, 2006).

By exploring the differences and similarities of I^2 attributes of programs, this thesis will produce a best practice model that can be realized to assist program managers in their effort to establish successful I^2 within a system of systems. In this chapter and Chapter IV, a review of the program I^2 attributes will be examined to reveal the successful and unsuccessful I^2 of system of systems. In Chapter V, a descriptive, normative and prescriptive model comprising a system of systems framework is proposed to provide categorization of attributes to introduce a best practice approach to applying I^2

to system of systems (Valerdi, Ross, & Rhodes, 2007). The methodology for this framework will be defined and applied in Chapter V. The information that will populate the models will be extracted from the research acquired in Chapters III and IV. In addition, heuristics by the authors are utilized which are in two forms: descriptive and prescriptive. Descriptive, which describes a situation but does not give direction on what to do, and prescriptive, which indicates what might be accomplished in a given situation (Maier & Rechtin, 2000).

This paper will present and I² framework for system of systems and recommend approaches to augment capabilities under evolving circumstances.

II. CROSSWALK OF C4I I2 DOCUMENTED “RULES”

A. INTRODUCTION

The federal government has highlighted the importance of integration and interoperability among physical systems and organizations. This is evident by the government requiring acquisition programs to follow specific mandates in two types of laws: statutory law and regulations and administrative law. Simply stated, Statutory Law consists of acts of legislatures and Regulatory Law consists of policies and procedures needed to administer the statutory laws passed by Congress and signed by the President (Knight, 2006). From these laws, the DoD has developed policy documents and specifications in the form of Directives and Regulations, respectively.

This chapter provides a crosswalk of these various documents to better appreciate and understand how the documents have helped the integration and interoperability (I^2) required for system designs.

B. BEHIND THE LAWS

In the early 1980s, military procurement had a series of public acquisition failures. Some of the more known problems were the \$435 hammer as part of the 34C Trainer kits, the \$640 toilet-seat cover for the P-3 aircraft, the \$659 ashtrays for the E-2C aircraft, and the much-publicized \$3,046 coffee maker for the C-5 airplane. Most of these are true, but further investigation of these costs changes the story (National Review, 1985).

The \$640 toilet-seat cover was actually the cost of the entire waste system onboard the P-3. Delta and TWA buy similar coffee makers for \$3,107 each, which makes the C-5 coffee maker look like a bargain (National Review, 1985).

These publicized procurements, which were part of various acquisition programs by the DoD, looked to be unethical and or wasteful procurements by Congress and others. Congress conducted numerous hearings with DoD senior leaders and Program Managers which resulted in hundreds of thousands of requests for information. Over the next

several years, Congress passed a series of laws, procedures, reviews, and reports that acquisition programs were required to follow and complete. As a result of this Congressional action, a new layer of bureaucracy within the acquisition timeline was established (National Review, 1985). As stated “Weapons programs must now manage a gauntlet of paperwork, which is burdensome and embarks more costs than are saved by the safeguards” (National Review, 1985). Vs. the actual quote: Weapons programs must now run a gauntlet of paperwork so burdensome and devious as to add far more to their cost than is ever saved by the safeguards.

The commitment by Congress to help manage and oversee acquisition programs has resulted in a number of laws that were intended to ensure systems would be designed for integration and interoperability but now these same laws are used as a shield by program managers to limit the system of systems integration that is now required as technology has advanced.

The following pages provide summations and analysis of I² in regards to the description and application of the laws.

C. STATUTORY LAWS

Extensive review of statutory laws was conducted to locate integration and interoperability references. These statutory findings were identified in the following public laws: Public Law 104-106 104th Congress, Feb. 10, 1996, Public Law 105-261 105th Congress, Oct. 17, 1998, and Public Law 107-314, 107th Congress, Dec. 2, 2002.

The Information Technology Management Reform Act of 1996 and the Federal Acquisition Reform Act (FARA) of 1996 were combined to become the Clinger-Cohen Act of 1996 (CCA) and is part of Public Law 104-106 104th Congress, Feb. 10, 1996. This law was designed to improve the way the federal government conducts procurement activities, requires the use of standards for better integration and increases the incorporation of commercial technology.

Appendix A contains just a few examples of how I² is used in this law.

D. REGULATORY LAWS

Regulatory law consists of policies and procedures required to administer the statutory laws passed by Congress and signed by the President (The University of Delaware Library, 2006). Appendix B provides an understanding of the regulatory laws, Joint Publications 1 and 6, Chairman of the Joint Chief of Staff Instructions, and DoD Instruction 4630.8, “Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS) governing I² required for C⁴I systems.

E. SUMMARY

As described in this chapter, there are many Statutory and Regulatory laws on the books today that ensure I². The catalyst for these laws in most cases was due to a few acquisition programs that did not perform due diligence regarding the spending of program funding or became the target of blame as a way of distracting attention from the real causes. Regardless of why each of these laws were written, they all seem to be reaction-based by Congress and others to “help” ensure the engineering and acquisition of future programs.

DoD has placed great importance on making our system of systems interoperable and integrated and requires that all new (and many existing) systems demonstrate they are interoperable with other systems and become certified as interoperable prior to fielding. DoD relies on the Joint Interoperability Test Command (JITC, part of the Defense Information Systems Agency (DISA)) to certify systems. In doing so, JITC reviews testing already conducted as well as assessments prepared by independent testing organizations. It may also conduct some of its own testing. The results are submitted to the Joint Staff, who validate the system’s certification. Systems are generally certified for three years—after which they must be re-certified.

Even with these laws in place with oversight by OSD NII and DISA, programs still perform minimum I² testing.

As of December 10, 2002, 24 of the 26 elements from the Distributed Common Ground-Surface Systems (DCGS) had been fielded without being JITC certified. Only after the United States Government Accountability Office published the report, 03-329 in 2003, “Steps Needed to Ensure Interoperability of Systems That Process Intelligence Data,” did the DCGS program office take corrective action toward these issues.

The design of warfighting capabilities through the use of net-centric I² systems will most likely not be accomplished by more laws and more GAO reports. Without a doubt, accountability and real programmatic penalties need to be defined and enforced to support I².

III. RESEARCH OF SUCCESSFUL INTEGRATION AND INTEROPERABILITY OF SYSTEM OF SYSTEMS DESIGNS

A. INTRODUCTION

This thesis will demonstrate the understanding of I^2 of systems across a system of systems design and how I^2 is applied to a system of systems framework.

At this point, a review of the different levels of system of systems is important to show how system integration can be defined and utilized in various ways depending on the type of system being integrated, process for integration, and the methods in which a system is bound for analysis. Through reviewing the work of Hobday, Davies, & Prencipe, 2005, Table 1 displays the spectrum of technical systems a program manager could face and have to accommodate system of systems issues.

<i>System Scope</i>				
4 Large Technical System of Systems	A4	B4	C4	D4
3 Product-System	A3	B3	C3	D3
2 Component/Subsystem	A2	B2	C2	D2
1 Assembly	A1	B1	C1	D1
	A Low-Tech	B Medium-Tech	C High-Tech	D Super High-Tech
<i>Technological uncertainty/novelty</i>				

Table 1. A Simple Typology of Technological Systems

The technical systems range from the scope of the system (physical nature and content) to the different levels of technology (low-tech, medium-tech, high-tech, super high-tech).

- Low-Tech = Systems that have no new technology required at any stage system integration is not required.
- Medium-Tech = Systems that have some new technology, system integration is unlikely to impact project.
- High-Tech = Systems that consists of recently developed technology, system integration is likely to pose issues.
- Super High-Tech = Systems that depend on new knowledge, skills, and materials are rare and rely on emerging technologies.

Program management should understand to which cell a program belongs in order to help bound the project and effectively utilize the model framework that will be presented in Chapter V. To this end, each type of system of systems would have a corresponding model framework that structures the system of systems categorized by a cell in Table 1. In applying the framework, some models would be similar in structure and content, some might be significantly different. Numerous examples are identified and developed in this thesis. As the programs are described in this chapter and Chapter IV, this table will be referenced for system of systems and technical level to provide a visualization to set the foundation for the system of systems framework introduced in Chapter V of this thesis.

In Table 1, whether the system of scope is assembly/low-tech (A1) or a system of systems/super high tech (D4), as technology changes, a system of systems approach enables people, technical systems, and organizations to effectively and efficiently adapt to change as needed in real-time to accommodate changing situations. A Homeland Security – SAFECOM (2008), system of systems brochure outlines the major concepts that are fundamental to successful system of systems:

- Systems are comprised of human, technological, and organizational components.
- Governance, technology, standard operating procedures, training, and utilization are important relationships.
- Independently operating systems can work with other systems and not lose their independence.

These are important considerations when examining the attributes of successful and unsuccessful I² descriptions in this chapter.

To this point, the various system scopes, level of technology, and concepts of importance in relation to the success of I^2 have been discussed. Another critical aspect of I^2 is the topic of “interfaces.” Standard (common) interfaces can help in integrating equipment, systems, and programs that are not compatible. This can provide operational, technological, and economic advantages as shown in Table 2 (SAFECOM, 2008).

Increased	Decreased
Operations by anywhere, anytime network to work upon authorization.	Reliance on proprietary technology enabling choice of vendors
Capability improved if system is based on standards to connect to other systems without compromising functionality.	Cost reduction because less costly customized interoperable solutions and training can be standardized.
Efficiency because the need for additional resources to improve interoperability decreases.	
Flexibility to upgrade without affecting other standard-based system.	
Capacity to expand is more likely with a standard interface versus proprietary.	

Table 2. Advantages of Standard Interfaces

Table 2 highlights the major advantages toward successful interfacing which supports interoperability that ensures integration. As Engebretson (2007) states, “When you have achieved that interoperability, the next step is integration, which we define as the ability for one device or software to be operated by another.” As the various programs are reviewed in this thesis, examples of criticality of interfaces will surface.

As much as interfaces are critical to system of systems I^2 , the topic of boundaries within and between systems requires discussion. Today we utilize custom and commercial off the shelf products that need third party technology for integration to occur. This makes it difficult to ensure I^2 , and when boundaries blur, it becomes even harder. This can be especially challenging if the boundaries begin to get fuzzy especially when dealing with the difference between a system of systems and a single, complex distributed system (Smith, Carney, & Morris, 2005). For example, a single shipboard diesel generator, as opposed to several diesel generators operating in parallel, would constitute a complex system - several parallel diesel generators being a system of

complex systems. The load following characteristics of a single unit is significantly different than the load following characteristics of several units in parallel. If this emergent behavior is not appreciated and understood, the system can easily be unstable (Turso, Ainsworth, Dusang, Miller, & Smith, 2007). Basically, determining whether a system is bound or unbound is critical. For a managed and engineered system, most likely the emergent behavior is not positive because the requirements dictate what the customer wants and most often the emergent behavior that surfaces from the system does not align with the customer requirements.

Figure 1 depicts the emergent behavior of bringing several systems together.

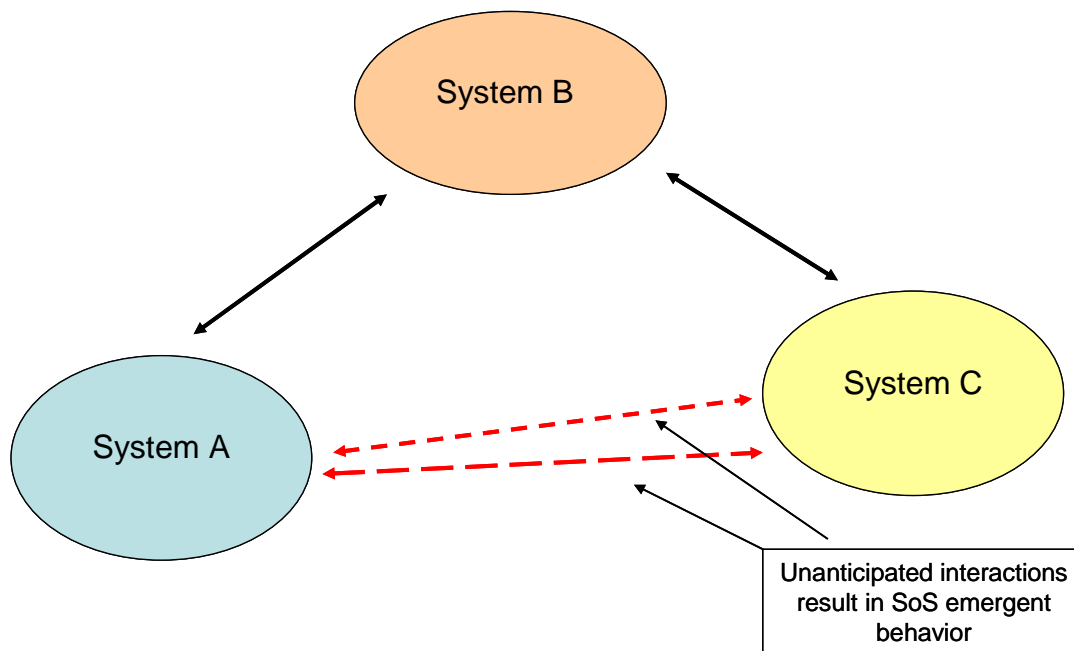


Figure 1. System of Systems – Emergent Behaviors

- System A interfaces with System B, bounded because the behavior is anticipated and stable.
- System C, new to the scene, interfaces with System B, bounded because the behavior is anticipated and stable.
- Emergent behaviors for the SoS due to unanticipated interactions between System A and System C result in an unbounded system of systems.

This is especially pronounced when incorporating human interaction among System A and C - essentially, System B is a human system component of a system of systems.

B. BACKGROUND

As stated in Chapter II, the pressure of funding, scheduling, and performance, for government as well as industry, amplifies the challenges of designing complex systems. Complex systems, once merged, result in joint system of systems, which enables the I^2 of a system of systems to be a collection of different systems designed for their own purpose and combined to produce a very large new system (National Research Council, 2007).

The idea of a successful system of systems depends on the perspective of the definition of “successful.” For many programs within the DoD, the definition of successful is related to spending the appropriated program funding on time or fielding the systems on time. With performance being the third part of program management, it is important to understand how other programs balance performance trade-offs as a function of successful system of systems I^2 .

A successful program from an I^2 perspective is a program that achieves seamless integration with other elements of a larger system of systems and provides timely and accurate interoperability to the system of systems capabilities. Improved coordination of initiatives and programs through authoritative oversight of related concepts, I^2 efforts are paramount to achieve an overall capability (Rogers, 2003).

Another perspective is how the DoD views system of systems integration as a method to pursue development, integration, interoperability, and optimization of systems to enhance performance in future battlefield scenarios (Pei, 2000). As seen in the DoD, this success is based on formal and derived requirements that ensure operational satisfaction of the customers from the Initial Operation Capability (IOC) and through the lifecycle of the system.

Without appropriate funding and scheduling for programs, performance, i.e., I^2 , can be compromised. The situation becomes more complicated when the DoD's

requirements process generates more demand for new programs than fiscal resources can support across many highly complex and interdependent programs. In addition, because programs are funded annually and department wide, cross-portfolio priorities have not been established. Therefore, competition for funding continues over time, forcing programs to view success as the ability to secure the next funding increment rather than delivering capabilities as promised (United States Government Accountability Office [GAO], 2005). All of these factors can contribute to the overall failure of programs.

Failure can often force a system's design back to the drawing board for correction to ensure performance. For system of systems failures, the correction can be difficult to quantitatively define as to who or what system(s) should incorporate the changes. Performance failures are not a bad condition in a holistic perspective. During a speech at the University of Delaware, Henry Petroski and Aleksandar S. Vesic Professor of Civil Engineering and Professor of History at Duke University stated, "Imagine that the Titanic had not hit an iceberg. Imagine that the Titanic had successfully reached New York. It would have been hailed as a tremendous success. What would have been the consequences of that?" (Parmley, 2006).

The challenges of successful I² design from a system of systems perspective can be related to the advancement in technology and the use of common off-the-shelf (COTS) items. The advancement of technology spurred the creation of companies and products that claimed to be integrated and interoperable. The number of COTS-based systems in the military has increased from 28% in 1997 to 70% in 2002. The issue is related to the COTS products with their own set of assumptions, which are not always compatible with other systems/components in the system of systems (Bhuta, 2007).

The purpose of I² C4I, a system of systems, is the robust and limitless capability of providing commanders with situational awareness. In contrast, the purposes of accounting systems are for business management, preparation for tax filing, analysis of buy and sell trends, etc. The purpose of C4I systems is to provide data to the right person, at the right time, displayed in the most effective manner for the end-user(s), which is the definition of right in this context. Like the definition of "successful," the definition of "right" can be part of the problem.

For C4I based system of systems, I² requirements are difficult to define. Requirements for system of systems are best defined from a user's perspective and from a capability perspective with traceable requirements to the next lower level down.

In most cases, C4I functional requirements are at a very high level. The lower levels, such as display and user interface attributes, of how a system's design is derived can be lost within the individual program and assumptions are formulated. For I², this level of detail assures multiple systems are all starting with the same system of systems requirements. This is normally not the case with new capabilities and new features being developed and fielded into system of systems environments that were not designed with these extended or enhanced capabilities.

The net-centric and joint warfighter is the way of the future, across individual programs and across the DoD services I² is the challenge of C4I for years to come. The success of this integration and level of interoperability will not come without failures. Leveraging the successful programs to the fullest extent possible is one of the keys to ensure I².

C. CRITERIA USED FOR SELECTION OF PROGRAMS

There are thousands if not hundreds of thousands of system of systems today within the DoD and commercial domains. Some are as complex as the phone system and others are as complex as the Space Shuttle or the sensor grid to detect worldwide missile launches. The approach used to evaluate some of these programs was based on multiple criteria, which highlighted the successes or difficulties to achieve integration and a high level of interoperability.

The commercial and DoD engineering environments are driven by different factors. For the commercial market, the engineering is based on time to market to capitalize on sales balanced against the cost of the product and the risk of brand name degradation or lawsuits over defective products. The driver is revenue. The building of a system that never fails is cost and time prohibited. Designing failure safeguards into systems that detect a failure is the most reasonable approach to systems designs.

Systems built by the DoD are driven by requirements developed by contractors, in many cases, approved, as the government requirements, by capability officers in the services and provided to the acquisition offices to implement the contract. The issues of stable and quantifiable requirements and funding that allow an I^2 design to be developed often initiates the problem of non-integrated and non-interoperable systems.

To understand the I^2 of a system design, consideration needs to be given to the maturity of the interfaces, data management, and systems hardware/software design. For example, to meet a requirement of fast and fixed latencies i.e., real-time, radar tracking, guidance alignment within a system of systems design, the engineering of the I^2 needs to be deliberate and well tested. There are other system designs that require I^2 to be near-real-time (i.e., common operating picture, chat) which are not reliant on rigid and fixed latency of communication or processes. Regardless, the system engineering to ensure I^2 in these systems (i.e., real-time or near-real time) is based on ensuring data is provided to the correct place in the correct format at the correct time. The programs selected for this thesis are based on innovative technologies and/or programs. The idea is to select programs that have or are being designed with I^2 verses experimental programs that are focused on technology advancements.

D. OVERVIEW OF PROGRAMS

These are successful programs that have, or will be required to design and implement, an I^2 system of systems design. To evaluate the success (or failures) of these designs, it is important to understand the scope and the drivers for each of the programs. The following describes five system of systems that have been successfully integrated and interoperable: NASA Space Shuttle and Apollo Program, Army's Future Combat System Program, Department of Transportation Railway Controls Initiative, DoD Joint Distributed Common Ground Systems Program, and an Enterprise's Learning Management System.

1. NASA Space Shuttle and Apollo Program

The NASA Space Shuttle program started in 1972 with a government contract to Rockwell International for \$2.6 billion. The I^2 of the shuttle and mission critical

requirements of the program drove much of the system's design. In 1976, the first test shuttle was rolled out to begin the Approach and Landing Test (ALT) program. The nine-month long ALT program involved ground and flight tests. These tests included the integration testing of various C4 equipment used in the handling and control capabilities required for atmospheric flight.

From the start, the Space Shuttle program used a systematic approach to the system of systems design that evaluated and tested the I^2 of the design from 1972 to the first earth orbit in 1981. System I^2 has been part of the program life-cycle support. In 2000, the Space Shuttle Atlantis introduced a host of enhancements including adaptation of the glass cockpit system, the use of radar to communicate with the ground, and a linked NASA satellite that allowed crews to transmit television-like pictures, voice messages and high speed data streams (Boeing, 2008).

The engineering and systematic approach to the design of the Apollo program was used with the Space Shuttle program as a basis for the program's systems engineering. In the fall of 2005, Massachusetts Institute of Technology (MIT) used the Space Shuttle program as a part of an Aircraft System Engineering course taught at MIT by Professor Aaron Cohen who was the Space Shuttle Orbiter Project Manager. The course offers a holistic view of the program from basic systems engineering, through risk analysis and management, and covers the key design drivers and decisions that attributed to the systems design and operational success of the program (MIT, 2005).

There are a number of interesting perspectives on I^2 and Systems Engineering within the Apollo Program and Space Shuttle program. Back in the 1960s during the Apollo program, NASA discussed "What is Systems Engineering?" Part of the NASA systems engineering process included making decisions in a timely matter. NASA's decision making process was based on sixty percent confidence level in the selection of the course of actions to baseline design solutions. From NASA's perspective, more than sixty percent confidence resulted in delayed decisions and most likely caused rework of designs (MIT, 2005).

An Interface Control Document (ICD) describes the interface(s) of a system and is key to the decision making process. There is a chicken and the egg paradox as it related to ICD and systems designs. This paradox in an ICD cannot be established until the system is designed but a system design cannot be completed until the Interface Control Documents is established. ICDs used by the Space Shuttle program include mechanic, electrical, functional, and data ICDs (MIT, 2005).

Requirements definitions were considered the hardest part of system engineering with interface management being part of the requirements definition effort. With a system of systems approach, the use of a matrix management of program engineering with checks and balances independent of the program is considered one of the keys to NASA's success of Apollo and Space Shuttle programs (MIT, 2005).

Some of the lessons learned include: establishment of interface working groups with mandatory participation, bringing in discipline experts when needed and not hesitating to go outside the program, government oversight of integrated testing with full-time Integration and Test leads required, monitored funding to ensure systems engineering activities are not cut during restructuring of programs, performing end-to-end testing early and defining integration leads before the design phase starts, giving adequate time to subsystem level testing and data system integration testing, and not short-cutting subsystems testing (MIT, 2005).

2. Future Combat System Program

The Future Combat System (FCS) is the Army's modernization program that integrates technology with combat teams and provides improved situational awareness and communications. FCS supports the asymmetric ground warfare that is within the Army's mission area. The FCS concept was initiated in 1999 with the timeline to deliver multiple capability fielding starting in 2008, equip the first brigade combat team in 2015, and equip fifteen brigades in 2030. As of April 2008, there are 75 FCS tests and evaluations ongoing across the United States. This program is on schedule while using a holistic system of systems acquisition approach (Army FCS Program Manger, 2008)

The I² of the FCS program is based on 18 networked warfighting systems which is the core of all FCS components. The networked systems model used by the FCS program allows the integrations of situational awareness, sensor fusion, and networked fires which are all capabilities that are part of Joint (service agnostic) warfare that relies on integrated solutions (GAO, 2003).

The FCS program established an overall System of Systems Integration Lab (SoSIL) network to support the interaction and integration of all the parts and pieces that makeup the FCS program. The software requirements verification and formal integration testing is key to the identification, troubleshooting, and isolation of integration problems. At the core of the FCS program is the FCS software suite with a mid-ware called SoSCOE.

SoSCOE stands for System of Systems Common Operating Environment. Some define it as the “glue” that ties FCS together as a critical FCS net-centric information environment. All C4I systems within FCS are required to have SoSCOE built into the operating systems. SoSCOE provides the internal FCS information delivery and management mechanisms; ensure interoperability services, security and information assurance services, and information discovery capabilities (Bassett & Emery, 2005).

FCS can be characterized as a complex adaptive system and, once fielded, will exhibit emergent properties that cannot be understood or predicted by studying the system elements in isolation. This assertion is based on four observations (Hartley, 2005).

- Warfighting itself is increasingly being recognized as a complex adaptive system. War is a multi-layered human enterprise. As such, it has many of the features studied in complexity theory work that is focused on social systems and economics.
- Modern war's focus on the role of information is generally increasing interconnectedness that will, in turn, tend to sharpen the effects of its complexity. Specifically, emergence, a key attribute of complex adaptive systems, is characterized in the complexity literature as an effect of system-level attributes related to information flows and distributed knowledge. Emergences is also caused by interactions of systems across system boundaries – this is best understood when system of systems are modeled using SysML, a graphical modeling language used in systems engineering, <http://www.sysml.org/>.

- The technological systems that FCS relies upon have very similar architectural elements to recognized complex systems. For example, communications and agent technologies are both current topics in complex systems research.
- The shaping of the FCS system of systems emergent properties and behaviors must be treated as an operational requirement. The basis upon which System of systems integration is possible may lie entirely in how well commonalities are exploited once determined.

The FCS will be a multi-functional, multi-mission, re-configurable system of systems that maximize joint inter-operability, strategic transportability and commonality of mission roles including direct and indirect fire, air defense, reconnaissance, troop transport, counter mobility, non-lethal and C² on the move. The goal of this effort is to develop a network-centric advanced force structure, quantify its benefits, and identify material solutions and technologies within the context of that force. It will also identify Doctrine, Operational, Training, Leader and Material (DOTLM) specific changes necessary as a result of the development of this network centric advanced force structure (Federation of American Scientists, 2000).

The FCS program has several progressive features, but also faces a number of challenges such as setting requirements, developing systems, financing development and managing the effort (GAO, 2005). The FCS concept shows the Army leadership is thinking innovatively to arrive at best practices to prepare for future Army operations. For example, Army leaders decided to include interoperability with other system requirements in the FCS design and design the individual FCS systems to work as part of a networked system of systems. Collectively, the system of systems could still provide an effective combat capability even if some of the individual system capabilities are lost or degraded (GAO, 2003).

This networked system model represents an improvement over the previous approach of first developing individual systems and later integrating which is an approach that often leads to schedule and cost growth. The system of systems approach provides program managers more flexibility to make trade-offs among the individual systems.

3. Rail Controls

Digital communication technologies are revolutionizing not only the telecommunications industry, but the railroad industry as well. Intelligent Transportation Systems (ITS) for highways and mass transit are based on these technologies, as are the new air traffic control and maritime vessel tracking systems. The military services, the major parcel delivery companies, pipeline operators, and police, fire, and ambulance services also use these technologies. The Federal Railroad Administration and the railroad industry are working on the development of Intelligent Railroad Systems that would incorporate the new digital communications technologies into train control, braking systems, grade crossings, defect detection, and into planning and scheduling systems. Intelligent Railroad Systems will improve the safety, security, and efficiency of freight, inter-city passenger, and commuter railroads (United States Department of Transportation [USDOT], 2002).

The highest priority of the Federal Railroad Administration (FRA) is the safety of the railroad system, the railroad personnel, and general public. Despite the improvement in railroad safety, there are still many railroad accidents of all types. With a goal of significantly reducing accidents and casualties, the FRA is aiming its research activities at addressing safety issues in each and every technological area that can reduce both the probability and severity of accidents (USDOT, 2002).

One technology being utilized is digital data link communications networks which provide the means for moving information to and from trains, maintenance-of-way equipment, switches and wayside detectors, control centers, yards, intermodal terminals, passenger stations, maintenance facilities, operating data systems, and customers. Data link communications will replace or supplement many of today's routine voice communications with non-voice digital messages and will effectively increase the capacity of available communications circuits and frequencies. Data link communications will utilize radio frequencies to communicate to and from mobile assets, and between locomotives in a train block using a variety of transmission media (owned either by railroads or commercial telecommunications carriers) to communicate between fixed facilities. These media include microwave radio, fiber optic cable, buried copper cable,

cellular telephones, communications satellites, and even traditional pole lines. With data link communications, the information is digitally coded and messages can be discretely addressed to individual or multiple recipients (USDOT, 2002).

In addition, the U.S. Government, through the Federal Communications Commission, has assigned to the railroad industry 182 frequencies in the VHF band (160 MHz) and six pairs of frequencies in the UHF band (900 MHz). The UHF frequencies are being used for digital communications; and some railroads have converted some of their assigned VHF frequencies from analog to digital communications. The conversion is expected to accelerate during the coming decade (USDOT, 2002).

Upon reviewing all the preceding examples, integration and interoperability are considered one of the major challenges to an Intelligent Railroad System. In the early 1990's, railroad chief executives considered the implementation of intelligent railroad systems, but decided instead to use available railroad capital for mergers and acquisitions, believing the mergers and acquisitions would yield a higher rate of return. The mergers, which resulted in four large railroads that carry over 90 percent of the rail freight in the United States, were not well executed and did not generate forecasted returns. Consequently, the major railroads do not believe they have the capital needed for investment in network-centric railroading and intelligent railroad systems. In fact, several of the large railroads are struggling to handle recent increases in freight traffic caused by the economic recovery, increased imports, the truck driver shortage, and highway congestion. However, they are investing in the construction of double-tracks, which provide capacity benefits in only a limited territory, rather than in tools to help them better manage their traffic flows over their entire network. Most senior railroad managers received their management experience in an environment of downsizing and cost-cutting; few have experience managing growth (Ditmeyer, 2005).

Railroads are currently not organized well for implementing intelligent railroad systems. The groups responsible for telecommunications and for train control systems are often in disparate parts of railroad organizations. Telecommunications staff often report to the information systems department, while train control staff often report to the track

engineering and maintenance department. Network-centric railroading requires that telecommunications and train control staffs either be amalgamated or have an extremely close working relationship (Ditmeyer, 2005).

Interoperability issues effect some but not all of the intelligent railroad systems. Locomotives equipped with radios using common frequencies and protocols, with common positioning systems, and with computers using common logic are necessary if Positive Train Control systems are to be implemented widely. Since the two types of electronically-controlled pneumatic brake systems are not interoperable, the railroad industry must decide which will be the industry standard. Other systems, such as tactical and strategic traffic planners, locomotive health monitoring systems, work order reporting systems, and wayside equipment sensors, do not require railroad industry agreement (Ditmeyer, 2005).

With the oversight and test facilities within the Federal Railroad Administration, a common governance and common criteria have been established for implementation an intelligent railroad systems. The FRA is able to test and certify individual systems that make up the system of systems capabilities of this high tech transportation structure. This ensures interoperability between systems given they have been tested in a real-world environment.

When new technologies are adopted and methods of operation change, it is only natural that some individuals, and even institutions, will be resistant to change. Those with knowledge of signal systems feel threatened by the adoption of a different train control technology. Some management will want to move the new, different, and more complete information through the existing stovepipes of the hierarchical structure, rather than directly to those managers and operators who can take immediate action based on the information. The United States military encountered this problem during Operation Iraqi Freedom (Talbot, 2004).

4. DoD Joint Distributed Common Ground Systems Program

The purpose of an intelligence sensor is to gather data from ground and surface systems. The categories of these sensors are celestial (satellite) or terrestrial airplanes and

unmanned ground sensors. The sensors provide raw data for the purpose of tracking, mapping and navigation, search and exploration, surveillance and reconnaissance.

In an operational context, these sensor systems consists of the data collection system and the ground terminal or ground system. Example 1): An Unmanned Aerial Vehicle (UAV) is the data collection unit and the ground system is the computer and communication suite that controls, re-directs, and gathers data from the UAV while in-flight. 2) A U2 or F18 aircraft is the data collection unit and the Tactical Exploitation Group system retrieves the data and performs data fusion on the raw data to create “Actionable Intelligence.”

Distributed Common Ground Systems (DCGS) is the Defense Airborne Reconnaissance Office (DARO) vision for the integrated architecture of all ground/surface systems. The DARO strategy is for DCGS to integrate the:

- Imagery Intelligence (IMINT) ground/surface systems in the Common Imagery Ground/Surface System (CIGSS) architecture,
- Signals Intelligence (SIGINT) ground/surface systems in the Joint Airborne SIGINT Architecture (JASA), and
- CIGSS and JASA architectures into DCGS.

DCGS will be completed by the addition of IMINT, SIGINT, and Measurement and Signature Intelligence (MASINT), which includes radar, infrared, acoustic, and nuclear intelligence (Pike, 2005).

The purposes of a DCGS test bed environment are to accomplish air-ground interoperability testing, support sensor development, evaluate CIGSS components, and support CIGSS architecture standards development in a mobile lab that could support rapid development, demonstration and evaluation of new capabilities. There are significant advantages to a mobile lab for sensor development, including co-locating with contractors to develop Interface Control Documents and risk reduction, co-locating with airframe contractors to verify sensor-to-ground station connectivity, and co-locating with government/contractors for final flight test Interface Control Documents verification. The test bed has an expanding role in SIGINT and MASINT disciplines and the test bed is involved in CIGSS level one and two certification programs.

The DCGS is a family of fixed and deployable multi-source ground processing systems that support a range of intelligence, surveillance, and reconnaissance systems such as national and commercial satellite systems, U-2, UAVs, and F-16 Theater Airborne Reconnaissance Systems. The U-2 Management Directorate at Robins Air Logistics Center provides upgrades of operational intelligence support systems to meet DCGS operational requirements for deployable ground stations.

Fielding of DCGS will be accomplished through the successful completion of a series of DCGS Migration Blocks. These blocks represent the planned fielding of new DCGS systems/capabilities and sites, and upgrades of existing functionality. No significant hardware or software development is envisioned for the DCGS Integration Support Contractor (DISC). The range of services will include, but not be limited to, system engineering, integration, planning, and maintaining an understanding of planned upgrades to Community ISR systems. A primary objective is to ensure current and future interoperability between AF DCGS and C² systems (Pike, 2005).

The Distributed Common Ground/Surface System-Marine Corps (DCGS-MC) is a subset of the Marine Air-Ground Intelligence System (MAGIS) network. MAGIS provides the capability to collect, process, analyze, fuse, and disseminate information derived from all Marine organic intelligence disciplines—including Imagery Intelligence, Signals Intelligence (SIGINT), Measurement and Signatures Intelligence, and Human Source Intelligence as well as national and theater systems. DCGS-MC meets specific Department of Defense requirements and connects intelligence professionals to multi-discipline joint, national and organic data sources, analytical assessments, and collection assets.

To meet the increased interoperability and data posting/sharing requirements levied by the Office of the Secretary of Defense (OSD), as well as the requirements for timely and accurate intelligence demanded by Expeditionary Maneuver Warfare, DCGS-MC will transform from a partially networked family of systems to an enterprise encompassing all of Marine Corps Intelligence Surveillance and Reconnaissance (ISR) assets and be fully interoperable with other Services, Agencies and COCOMs (HQMC, 2004).

This enterprise solution will be called the Marine Corps ISR Enterprise (MCISR-E). MCISR-E is an enterprise that encompasses the entire Intelligence Cycle in order to better assist the USMC operational planning and decision-making processes (HQMC, 2004).

There are many pitfalls to I² of DCGS. ‘Who leads the effort?’ seems to be a common question with few answers. How to avoid protected territories of past programs is another roadblock to I² because every program seems to create new infrastructures.

As the network provides great connectivity and multiplying effect, it also provides a common path for enemies to access all of our systems. As systems connect to the network, whether local or dispersed, they publish their services. These services provide everything that the other system needs to make use of that service. A key point for this approach is that both the service consumer (client) and service provider (server) parts of the software are developed, tested and validated by the same contractor (the service provider). This is thought to drastically cut down the issues of interoperability due to incorrect implementation of the ICD. Also, since this approach assumes a standard network connection, it is much simpler and cheaper to implement (no custom hardware or connectors).

DCGS is striving for a single service model and single contractor, with a common concept of identity that allows services to create one architecture to be utilized by services from a different architecture. This should allow C4ISR applications to be common among these architectures (Morris, 2006).

The Distributed Common Ground System (DCGS) Integration Backbone (DIB) is an open-architecture designed to provide interoperability at the data services level for all the U.S. military and coalition services. The DIB is a set of common interface standards and tools that allow seamless intelligence data sharing and collaboration across the C4ISR enterprise of enterprises, delivering the right information at the right time to maximize operational effectiveness (Morris, 2006).

5. Learning Management System

A Learning Management System (LMS) enables the delivery, management, and administration of training for an enterprise. It supports an integrated approach to training by combining computer based and traditional classroom training. This system of systems provides centralized content, student management, and reporting in one technology package. One of the key attributes to a LMS is the open interface that enables the ability to download employee information and upload performance and completion data. These interfaces support basic integration of computer language formats as XML and industry standards, including IMS, SCORM, and AICC (Robbins, 2002).

For the purpose of this thesis, the enterprise and manager will not be named since it does not impact the thesis results. The manager for “Education Systems” of “Enterprise A” was interviewed to discover if the implementation of the LMS for that enterprise was successful in the areas of I² both on the technical and human side.

The two business drivers of a LMS for this enterprise were 1) cost economies of scale and 2) cultural aspect by bringing divisions together to form a whole-one enterprise.

The overall purpose was to maintain the employee training records and certification. This enables movement of personnel and training across divisions; therefore, interoperability on the human side. Basically, if an employee goes to another sector within the company, their records are in sync. The benefit of “one” place for all information is because each division has an interoperable system which feeds into a larger system. The interviewee pointed out this seamless approach could happen because of two factors: 1) the high tech culture of this enterprise was conducive for this type of large scale software application and 2) decision was made in the design phase not to modify the software but instead modify business processes. The second factor was critical in the entire lifecycle of the project.

The manager stated the upfront driver for I² as a capability was the legacy system did not contain I². Therefore, the system was very inefficient with large amounts of rework. For example, certifications and education were located into two separate systems along with a manual effort of matching training with qualifications. This process also had records located across the company without any central authority.

To ensure I², a governing committee was established that provided oversight to all aspects of the requirements, purchase and operations of the system. It was, and still is post-implementation, an integrated effort from all divisions of the enterprise. Examples of the current I² are:

- a nightly feed of elearning information is captured through an automated and standardized process throughout the enterprise and
- the LMS has been integrated with SkillSoft, a third party elearning software system, (<http://skillsoft.com>). This was seamless because the SkillSoft integration was a bidding requirement from the beginning of the project.

There are future plans to integrate with other third parties because the interface is present and can be modified as needed. Using LMS structure provided I² that provides efficiency, accuracy and effectiveness. In essence, both I² was successful on the technical and human side of this project.

E. SUMMARY

Each of the programs described within this chapter has challenges and approaches to ensure achievable I² solutions. The requirement for I² comes from the need for human safety, efficient situational awareness, or seamless intelligence data sharing. The hurdles in many cases are related to implementation strategies.

The current implementation strategies are 1) a firm governance structure from the use of a single contractor or a single program office (e.g., NASA, FCS), 2) funding and contracting to a single I² company for other programs (e.g., DCGS), and 3) implementation of very simple I² solutions.

The programs described in this chapter had I² networks and sustained lab facilities to test and evaluate new spinouts, modules, or new elements of the larger system of systems capabilities. The funding for these efforts were not discussed because funding of facilities for system of systems testing is considered part of the overall program requirement to identify issues, correct the problem, and retest to ensure I2.

The idea that I2 systems can be legislated, as demonstrated in Chapter II, or just naturally occur is not the case. This chapter highlights several successful programs relating to I2 and the knowledge and heuristics gleaned from research and interviews. This analysis will be synthesized in Chapter V through a descriptive, normative and prescriptive model comprising a system of systems framework to provide categorization of attributes to introduce a best practice approach to applying I2 to system of systems (Valerdi, Ross, & Rhodes, 2007). The methodology for this framework will be defined and applied in Chapter V.

The challenge remains..... How to integrate and create interoperability between systems that are independently developed?

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESEARCH OF UNSUCCESSFUL INTEGRATION AND INTEROPERABILITY OF SYSTEM OF SYSTEMS DESIGNS

A. INTRODUCTION

In Chapter III, the focus was on researching various system of systems programs that dealt with large scale system of systems designs that were successful in I² for a number of reasons. The lessons to be learned from successful system of systems I² are key attributes in which a future system of systems I² should look to repeat. However, the lessons learned from examples of non-integration and non-interoperability are equally as important.

The research in this chapter highlights some of the key attributes of non-integration and non-interoperability seen in various system of systems designs. The identification of these attributes in a system of systems design should be an alarm to leadership that problems within the design need attention and there is a high risk of I² issues. The following describes four system of systems that have been unsuccessful: Combat ID, Coast Guard Deepwater Program, Unmanned Air Vehicles, and Enterprise Systems.

B. OVERVIEW OF PROGRAMS

1. Combat ID

Within the fog of war, the enemy is shooting at combat troops and the combat troops are returning fire. This battle space includes ground-to-ground, ground-to-air, air-to-ground, and sea-to-ground/air. Within this battle space, the need for accurate, near-real-time situational awareness is required. The location and movement of both the enemy and friendly forces allows for effective and proportional discharge of deadly force.

The issue of accidental firing on friendly combat troops has been problematic for many years. Within the early history of warfare, the two sides of a conflict would enter the battlefield with the troops lined up in an open field with bows and arrows, hot oil

slight shots, and cannonball projectiles. The asymmetrical warfare of rapid attack, displacement, diversion tactics, etc has risk of accidental firing one's own forces. This force-on-same force attack is termed "friendly – fire."

In 1995, which was the 50th anniversary of World War II, the Defense Science Board (DSB) issued a report that examined the issue of friendly – fire and if/how a Combat Identification (Combat ID) could be implemented. The report concluded there was not a crisis in Combat ID calling for extraordinary action (DSB, 1996). Given the lessons learned from both Gulf Wars, war fighters with theater experience may not agree with this finding.

This same report identified the need for better target recognition capabilities in radars on surveillance platforms, increased distributed situational awareness in a netted communication environment, and new technology for surveillance, processing and reconciling differences in situational awareness (depiction of common operating picture) and combat ID.

The report did not look at Combat ID issues as they relate to dismounted warfare in door-to-door large-scale mobile warfare operations. It is important to recognize that the Iraq and Afghanistan operations are based on dismounted warfare. Given the DSB report did not address what is now the main warfare op (i.e., dismounted), some of the conclusions in the report may need to be revisited. From 1996-2001, \$12.92 billion was spend on C4I but Combat ID funding has been significantly lower. An overriding observation is that a heavy investment and continued spending is an important requirement for Combat ID for the future (DSB, 1996).

The negotiated position by the United States and North Atlantic Treaty Organization (NATO) partners regarding Combat ID is to participate with NATO Standardization Agreement (STANAG), which determines the processes, procedures, terms, and conditions for military or technical procedures or equipment between the member countries of the alliance. This partnership will reflect specific Combat IDs implementation strategy for both Air domain and Ground domain combat areas but with no commitment to upgrade to a single Combat ID. Ground combat is the most serious

Combat ID shortfall listed in the report (DSB, 1996). This commitment for commonality of a Combat ID method(s) while providing limited specific systems recommendations or standards does not provide any significant path forward to unified efforts in this area.

Coalition partners in the Second Persian Gulf War, i.e., the Iraq War in 2003, continue to have integration problems with the United States. Great Britain deployed a prototype Combat ID system successfully in 2001. However, after significant time and cost spent by the Ministry of Defense (MoD), the British force had difficulties communicating effectively with their allies, in particular the United States (Kablenet, 2007).

General James Conway, Commandant of the United States Marine Corps commanded Marine ground forces during the Iraq war in 2003. With experience from the First Persian Gulf War in 1991, basic identification systems were hastily fielded just prior to the Iraq War. From General Conway's perspective, friendly fire incidents were "probably my biggest disappointment of the war" (Peck, 2003).

The Army, Navy, Air Force, Marines, and Coalition Forces have all been developing electronic based Combat ID solutions with few integrated or interoperable solutions. The NATO standard that uses millimeter-wave signal is not interoperable with United States Forces. The Army's design that uses a radio based Combat ID does not support Marine Corps rifle squad needs with critical firing times.

With many low-tech visual panels, cloth panels, glo-tape squares and the like, the Army has been tweaking its existing Combat ID equipment from these implementations into the digital age with a slightly different millimeter-wave form solution mostly focused on their track vehicle (i.e., tanks) solutions. This high tech solution is estimated to limit casualties to no more than a 3 percent loss. Friendly fire in the first Gulf war is estimated at 17 percent of all casualties. During World War II, friendly fire accounted for about 20 percent of the casualties (Peck, 2003). Based on these percentages, even though they do not concur with the Defense Science Board report, it shows that further investigation is required to improve interoperability of Combat ID solutions.

A key finding shows that a lack of I² for Combat ID to resolve friendly fire seems to be based on political pressures, which has resulted in suboptimal, non-integration solutions by multiple DoD Armed Forces and with limited interoperability between these services solutions. This system of systems solution is lacking a cohesive coordinated requirement, operational context, and unified commitment to work together.

Combat ID is at the forefront of all coalition military operations around the globe. With continuously changing battlefield environments, rapid evolution of war fighting concepts and tactics, and new coalition partners joining the fold, the location and recognition, and identification of one's own forces to reduce fratricide has never been more vital.

As General Conway, USMC, noted, "Whoever comes up with a solution for friendly fire, will be very rich, indeed. Because it continues to be something that we see happen in the US military, and it's really something that we've got to stop" (Peck, 2003).

2. Coast Guard Deepwater Program

Prior to the 1980s, the Coast Guard had few acquisitions of new ships or aircraft. The aging fleet of 90+ cutters and patrol boats, 107 aging planes and helicopters, and few C4I upgrades over the years resulted in technical obsolescence. This was the genesis for the Coast Guard to initiate the Deepwater acquisition effort in the late 1990s. The acquisition strategy was based on a single, performance-based contract with all design, building, and systems integration to be accomplished by the contractor in a Lead Systems Integrator role. Total funding requested in FY02 exceeded \$320.2 million with a total acquisition cost estimated at \$24.23 billion (GAO, 2004).

The decision by the Coast Guard to hand over all design, build, and systems integration responsibility to a contractor was based on a belief that the government workforce within the Coast Guard was unable to support the size and complexity of the Deepwater program. It was also thought that a performance based contract allowed for the best (optimized) common integration across a wide range of platforms.

By 2003, the Coast Guard through fair and open competition selected a contract winner. The contractor was awarded a unique indefinite delivery, indefinite quantity contract for 5 years with the option for five more, five year each extensions.

The Deepwater program is a large system of systems acquisition. The integration of advanced ship control and monitoring to reduce ship crews, modernization of C4I systems suites, and seamless logistics support for all components seemed to support this system of systems approach.

As early as 2004, many outside observers external to the Coast Guard started to raise questions of concern. In March 2004, the GAO -04-380 report criticized not only the effectiveness of the contractor and related competency to deliver a quality product but questioned the “hands-off” management and engineering decision making by the Coast Guard (GAO, 2004).

The initial warning signs of a troubled acquisition program and a failing system of systems integration became real in 2005. The contractor completed the integrated new C4I equipment to provide enhanced capabilities and overhauled 49 legacy patrol boats to extend the end-of-life for these surface craft. Upon inspection and after operational testing, significant structural design flaws and insufficient C4I capabilities that failed to meet the documented post 9/11 operational requirement were discovered (Department of Homeland Security, 2007).

Similar problems with the National Security Cutters (NSC) were discovered in November 2006. With the design and integration failures building, the Department of Homeland Security, Inspector General, Justice Department, General Accountability Office, and a wide range of open news organizations proceeded to examine the Coast Guard and the Deepwater program.

A point of interest for C4I system of systems design is the contract focus to utilize commercial equipment and software as much as possible (Anderson, Winterstine, 2003). The integration of Commercial Off-The-Shelf (COTS) is viewed as plug and play with little or no systems I² testing required. The underestimation of the engineering involved for I² of a COTS solution causes much of the failures in this area. The utilization of

COTS should advance the C4I design given there is not a need to build from scratch communication hardware, computers, etc. Often a critical aspect in the process is to create an architectural C4I baseline with COTS products.

Another interesting point is that with the urgency to field new and improved capabilities in the aftermath of 9/11, the Coast Guard and Department of Homeland Security seemed to look for the quick and easy solution instead of a solution that provided balanced cost, schedule, and technical risk. Like with many military programs, the cost and schedule of programs are underestimated to “win” the program at the expense of reducing technical capabilities, which limits I². The Coast Guard developed an aggressive modernization and acquisition program in scale (cost) and urgency (schedule) in a single contract with minimal internal review. Additionally, they only provided a brief time period to solve unexpected problems and did not follow the system engineering process to baseline the level of achievability of the schedule.

In retrospect, the decision by the Coast Guard to empower the contractor to do a majority of system design and integration allowed for minimal technical involvement by the government. The contractor and government have very different motivation factors. The contractor is motivated by contract awards, incentive fees, and corporate profit. The government is motivated by securing funding, successful program execution, maintaining an industrial base, and balancing acquisition risk management of cost, schedule and performance. This is further complicated by the workforce comprising of government officials moving into the industry workforce and vice versa. Regardless of the potential conflict of interest by government personnel or unethical behavior by individuals, there was a lack of involved competent program managers and systems engineers in the day-to-day operations and approval cycle. With the acquisition strategy used in the Deepwater program, the government oversight for all aspects of the design, development, testing and fielding of the system of systems design was clearly missing the aspects of a legally binding program or technical authority responsibility.

In response, the Coast Guard and the Deepwater program made significant changes in late 2007. These changes included the “in-sourcing” of the systems integration role with the government for all related Deepwater development and the hiring of

additional government workforce with both the training, education, and experience to effectively support the systems integration and ensure interoperability across platforms. In addition, the use of proper design standards and a balanced and realistic design schedule with upfront systems engineering activities was base-lined. In the FY09 funding request by the Coast Guard, \$990.4 million for Deepwater was approved. The cost of the flawed acquisition strategy and re-design, re-engineering the C4I suites is estimated at well over \$500 million to date for the total Deepwater program (Congressional Research Service, 2008).

3. Unmanned Air Vehicles

The history of Unmanned Air Vehicles (UAV), unpiloted aircraft, is longer than one might think. From a warfare perspective, UAV were as simple as a Douglas Archibald surveillance kite, Figure 2, which took the first successful aerial photographs in 1883. Thereafter, this UAV was used extensively during the Spanish-American War of 1898 and provided critical information to United States forces.

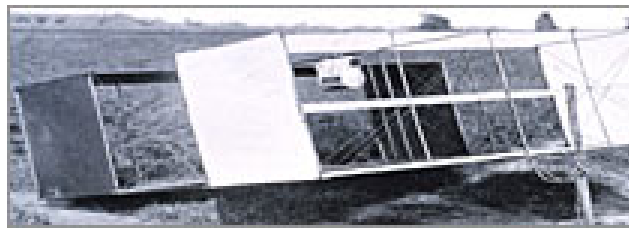


Figure 2. Douglas Archibald Surveillance Kite 1883

The idea for a UAV to be more than surveillance was conceived by Adolf Hitler in the early days of World War II. The Vergeltungswaffe-1 (English translation – Revenge Weapon) or V-1, Figure 3, was designed by manufacturers Fieseler Flugzeugbau and Argus Motoren and was ready for service in 1944-45.



Figure 3. V-1 designed by Fieseler and Argus Motoren

Launched from catapult or host aircraft, the V-1 had a powerful thrust pulsejet engine that had a range of up to 150 miles with a 2,000-pound bomb payload. The brain of the V-1 was a simple autopilot and a gyrocompass that provided vector control to a pre-programmed altitude and speed. Once the V-1 was launched moving in one direction from the catapult, it would climb to its set altitude until a pre-set counter/timer triggered the arming of the warhead and directed the V-1 into a steep terminal dive (Luftwaffe Resource Center, 2008). Although the success of the V-1 is questionable, this was the start of powered un-tethered UAV designs and birth of the cruise missile (http://en.wikipedia.org/wiki/V-1_flying_bomb).

Following World War II, many countries continued the advancement of air-breathing UAVs through the 1940-1970s that supported operations during the Cold War and the Vietnam War. Also following World War II were the advancements of other technologies that took UAVs from a “point and shoot” (one direction) system to computer-based remote control and real-time transmitter that are characteristic of today’s UAV.

The development of small and lightweight UAVs like the Scout and Pioneer by the Israel military overcame many of the challenges that limited UAVs. The use of the Scout UAV by the Israelis in the early 1980s was extremely successful during the Bekaa Valley conflict between Israel, Lebanon, and Syria. The inexpensive Scout UAV using real-time imaging via a microwave data link from a stabilized 360-degree video

surveillance camera mounted on the belly of the Scout, located Syrian missile sites and allowed Israeli bombers to destroy all but two of the 17 launch sites (<http://www.israeli-weapons.com/weapons/aircraft/uav/scout/Scout.html>).

The aggressive development of UAV capabilities has placed these systems into critical warfighting, border patrols surveillance, and humanitarian functions around the world. However, the I² challenges of incorporating UAVs into the high-tech military arsenals had problems.

UAVs range in size from arm-launch planes to the size of small commuter planes. The success of UAVs in warzones has proposed the use of UAVs in other mission areas. The number of UAVs has increased from fewer than 100 six years ago to 3500 in 2006 with about 700 operated by the Coast Guard, NASA, Homeland Security, and the National Oceanic & Atmospheric Administration (USA Today, 2006). The I² of UAVs developed into un-managed or semi-managed radio environments causing significant problems and crashes.

Modern military warfare has continued to push the digital frontier to the tactical edge and beyond. A common problem seen during both Gulf Wars has been the radio interference and the disregard of spectrum management that has hampered United States UAV operations. In 1987, the GAO report 87-42 titled “Radio Frequencies – Earlier Coordination Could Improve System Use and Save Cost,” documented the lack of DoD management of frequency spectrum in radios, radars, and other critical C4I systems which includes UAVs (GAO, 1987). In a follow-on GAO report 01-604 in 2001, the GAO found the DoD has taken steps to ensure program managers identify and address potential interference problems early in system development (GAO, 2001). For example, the new acquisition guidance establishes procedures that require all new weapon systems acquisition programs to be reviewed for potential electromagnetic and spectrum management problems as they go through the acquisition process.

Even today, the problem of I^2 of UAV remains an issue. Based on a report in NETWORK WORLD, May 2008, an analysis of information from the DoD on 199 UAV crashes that occurred during from 2003-2007 of operations Enduring Freedom and Iraqi Freedom indicates issues with UAV reliability and lack of protected radio frequency spectrum.

4. Enterprise Joint System

Enterprise-wide integration dates back to the 1950s and 1960s (Alsene, 1994). Throughout the 1990s, leading researchers have claimed that integration is the most distinguishing characteristic of a successful large-scale system. As seen in Figure 4, (Singletary, 2002), integration has evolved from the simplistic computer program to complex Business-to-Business initiatives.

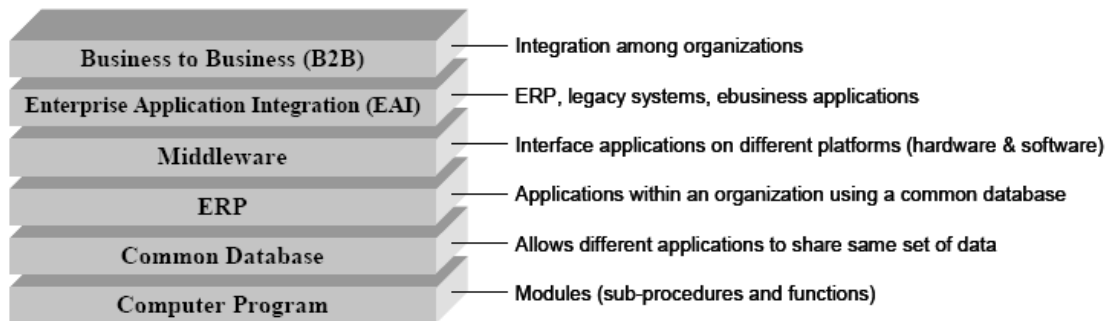


Figure 4. History of IT Integration

Since interoperability supports integration, it appears that I^2 is intimately related to enterprise systems such as Enterprise Application Integration and Enterprise Resource Planning (ERP) (Singletary, 2002). The program described below involves the aspects of I^2 surrounding an ERP system and a merger of two sites to form one company.

Since it does not impact the results of this thesis, the enterprise and manager will not be named due to confidentiality. The manager for “Organization Change” of “Enterprise C” was interviewed to discover if the implementation of a Joint System for that enterprise was successful in the areas of I^2 both on the technical and human side.

The two business drivers for the Joint System were 1) cost economies of scale (cheaper to have one system where business transactions result in the same data capturing) and 2) cultural aspect by bringing two companies together (merger) to form a whole (One Enterprise). At the time, the culture was not conducive for bringing the legacy systems into a new system of systems. Since the enterprise and its environment have a major impact on whether a system is successful in meeting its mission, this was an important factor in the success of this particular software implementation (National Research Council, 2007). Historically, the two sites were competitors within the industry (Site A/Site B were merged into one). A new name was given and for the purpose of this thesis is named Site C. There was a physical distance of approximately 100 miles between companies.

In regards to stakeholders, it was noted the stakeholders included upper and middle management but not end-users. An executive committee was formed with power of authority. This committee, which comprised the stakeholders, met weekly. Funding was stable for this project. Requirements for I² were not formally written or part of the front-end design of the implementation.

The overall purpose to developing an Enterprise Joint System was to utilize the existing legacy system at Site A, one ERP system that included a Human Resource component, by modifying it to accommodate more end-users (3,000 to 6,000) from Site B which resulted in a Site C ERP system that included both Human Resources components from Site A and B. The merger of these two sites created Site C, Figure 5.

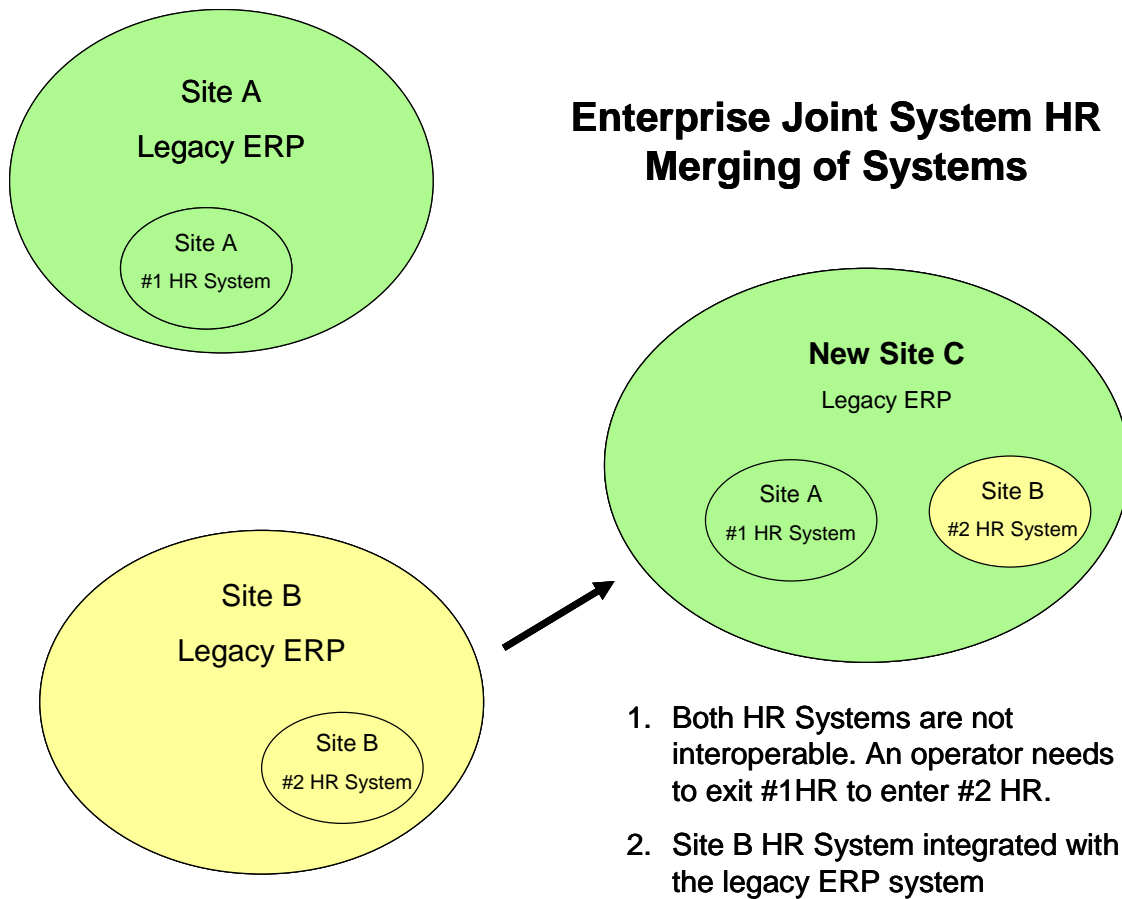


Figure 5. History of IT Integration

The legacy ERP system at Site A included the #1 HR system. The legacy ERP system at Site B included the #2 HR system. The Site B #2 HR system was integrated inside the Site A legacy ERP system; thus, eliminating the Site B legacy ERP system. Although integration occurred, the Site A and Site B HR system were non-interoperable. An operator needs to exit Site A HR system in order to enter and operate in Site B HR system. The result is the third circle, New Site C, in Figure 5. The interviewee pointed out the transformation of this system of systems enabled the enterprise to have one ERP for seamless integration across the division. The business was managed the same way on both sides of the house; same metrics, same terminology, same processes, etc. This made the transformation easier from a business perspective.

On the technical side, this implementation was successful with integration because the HR System for Site B integrated seamlessly into the ERP system. However, the interoperability was not successful because once Site A and B HR System was embedded into the ERP system the two sites could not exchange information. The operator has to abort Site A in order to enter Site B.

On the human side, the integration did not occur and interoperability was difficult between Site A and B. Since this was the merging of two companies, Site A end users knew their business processes but not the business processes of Site B. This was a challenge because Site A was in charge of developing and delivering training. For example, thirty subject matter experts from Site B were continuously interviewed to capture the entire picture of the legacy system. There was not any integration between functional areas or even within the functional area of Site B, which created a more complex challenge for Site A to create with a work breakdown structure. A job task analysis was not available to be used by Site A. Therefore, the fact that end-users would have different positions that possibly required new knowledge, skills and abilities was not acknowledged in the front-end to provide a workflow to support training of end-users. The mitigation plan developed was to have Site A subject matter experts work at Site B for months post go live to assist for up to 12 months.

In retrospect, it seemed to the stakeholders that I^2 would naturally occur in a successful manner both on the technical and human aspect. It needs to be realized that a system might work but the day-to-day business will not necessarily work. Often at the tactical level, it seems the end user understands the realities and importance of I^2 integration more than other stakeholders. Therefore, in the concept design phase end-user representation is critical to I^2 .

C. SUMMARY

Within the DoD and industry, there are thousands of system of systems programs that have requirements to be I^2 with other legacy systems or other programs. The programs described in this chapter are a small sample that highlights the system engineering struggle with the I^2 of a system of systems capabilities.

Other research suggests that programs are dysfunctional because of software issues only. Although this thesis addresses a system of systems viewpoint, it is important to pause and review, based on the samples provided in Chapters III and IV, the common challenges of I^2 relating to software. Independent analysis of more than 280 federal, state, DoD, and commercial software-intensive programs were evaluated for characteristics related to direct or indirect common failures observed in system acquisitions that had difficulty with delivering products on time and on budget (Evans, Abela, & Beltz, 2002). The seven common characteristics are listed below and how these same characteristics could be related to I^2 failures:

- Failure to apply essential project management practices. Many project managers did not utilize project scheduling, configuration management, and proactive risk management. From an I^2 perspective, this could reflect negatively toward having sufficient time and base-lining of interfaces to ensure the project meets the I^2 requirements.
- Unwarranted optimism and unrealistic management expectations. Some managers view components of a project through rose-colored glasses, remain in denial, and assume problems will be naturally resolved. Rarely does one find the integration of systems occurs naturally. Unless expectations are set upfront regarding the challenges of the I^2 to other systems, it is also unrealistic that more than one system will perform seamlessly with other systems.
- Failure to implement effective software processes. It seems programs fail to follow development processes for a number of reasons. Regardless of the facts that cause this adhoc approach, this leads to a high reliance on staff expertise. The factors that go into I^2 can be very process oriented if the project follows such an approach. The top-down design of the operations, activities, functions, interfaces, protocols, data, etc. can lead to I^2 each and every time if followed.
- Premature victory declarations. Given that schedule is a key component to a successful program, premature declarations of completion should not happen. Success should not be declared until all the products are completed and tested because often quality and reliability suffer at the expense of meeting a deadline. For example, the Joint Interoperability Test Command (JITC) is responsible to test all programs that utilize standard interfaces to specific global nets or systems. Many times programs that successfully perform JITC Testing of standards compliance believe they are ready for fielding yet these same programs can/do fail to be I^2 once fielded. Therefore, it takes more than standards to be I^2 .

- Lack of program management leadership. There are two types of leadership problems: managers with engineering and no management experience, and managers with management and no engineering experience. Without a blend of technical and managerial competency, I^2 from a system of systems perspective will mostly be lacking.
- Untimely decision-making. Some managers avoid making time-critical decisions until it is too late. Unless the critical interfaces that support the I^2 are defined and base-lined early in the concept design phase, the risk of non-integration; therefore, non-interoperability risk is high.
- Lack of proactive risk management. Many projects do not effectively utilize risk management. The distinguishing of the best programs with the best managers is how well they contain their failures. The I^2 of a system of systems capability is considered by many a significant effort. The “failures” identified during development and testing of a program should be looked at as the “successes” to resolve I^2 issues before the program is fielded. The I^2 of a program and the resolution of non-integrated and non-interoperability should be a high priority focus once identified by the project manager.

In Chapters III and IV, a review of the program I^2 findings examined the successful and unsuccessful I^2 of system of systems. In the next chapter, a descriptive, normative (notional) and prescriptive model comprising a system of systems framework is proposed to provide categorization of attributes to introduce a best practice approach to applying I^2 to system of systems.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SYSTEM OF SYSTEMS INTEGRATION AND INTEROPERABILITY FRAMEWORK

A. INTRODUCTION

In review of the system of systems highlighted in this thesis, according to Gholz, 2002, metrics available to compare system integration capabilities are limited. Therefore, program managers have difficulty assessing the technical and human capabilities needed for successful I². One set of metrics that evaluates the software engineering and system engineering level is the Capabilities Maturity Models developed by Carnegie Mellon University's Software Engineering Institute (SEI), a research Federally Funded Research and Development Center (FFRDC) (<http://www.sei.cmu.edu/>). These models are based upon an enterprise's dedication to following procedures to manage complex projects while maintaining control of documentation and interfaces at the component/subsystem level. For a program manager, these models may not be appropriate for assessing the I² of system of systems nor providing a proactive design approach for I² during the concept design phase of the product development lifecycle. A version of Table 3 presented early in Chapter III is now revised and presented to visualize how the programs from this thesis fit into this framework of system of systems at the High-Tech and Super High-Tech levels (Hobday, Davies, Prencipe, 2005).

<i>System Scope</i>				
4 Large Technical System of Systems	A4	B4	C4 - NASA Shuttle and Apollo program - Deepwater	D4 - Future Combat System - Rail Controls
3 Product-System	A3	B3	C3 - Learning Management System - Common System - Unmanned Air Vehicles	D3 - Distributed Common Ground Systems - Combat ID
2 Component/Subsystem	A2	B2	C2	D2
1 Assembly	A1	B1	C1	D1
	A Low-Tech	B Medium-Tech	C High-Tech	D Super High-Tech
<i>Technological uncertainty/novelty</i>				

Table 3. A Simple Typology of Technological Systems with Nine System of Systems

Thus far, explanation has been given for the various system scopes, levels of technology, concepts of importance, interfaces, and boundaries in relation to the success of I^2 that has occurred. In addition, through review of system of systems in Chapters III and IV, results of key attributes were identified that result in an I^2 system.

B. SYSTEM OF SYSTEMS I^2 FRAMEWORK

In this framework, the attributes of system of systems I^2 through descriptive, normative (notional) and prescriptive models will provide categorization to introduce a best practice approach to applying I^2 to system of systems. The three models, descriptive, normative and prescriptive, form a system of systems framework that as proposed by the authors can provide a categorization of attributes to introduce a best practice approach to applying I^2 to system of systems. The framework, provided in Table 4, is an extension of the work developed by Valerdi, Ross, & Rhodes, 2007.

For the purpose of this thesis, a descriptive model represents the actual behavior and the reality of a system of systems program utilizing I^2 . The descriptive model describes a situation but does not give direction on what to do. The normative model

represents the standards and is a comparative measurement against the descriptive model providing a methodology for a gap analysis. Depending on the nature of the system of systems program analyzed, the normative models applied may be generic in nature or may require customization. This information formulates the prescriptive model, which provides specific recommendations to achieve the ideals referred to by the normative (notional) model. It indicates what might be accomplished in a given situation (Maier & Rechtin, 2000). The descriptive, normative and prescriptive attributes for these models are based from selected system of systems highlighted in Chapters III and IV.

System of Systems I ² Framework		
"Name of System of Systems"		
Descriptive Model		
	Integration	Interoperability
Purpose/Capabilities		
Scope of I ²		
Stakeholders		
Funding		
Schedule		
Technical Requirements		
Human System Integration		
Criticality of Interfaces		
Seamless Operation		
Compare Descriptive Model Against Normative Model		
Normative Model (Notional)		
	Integration	Interoperability
Purpose/Capabilities		
Scope of I ²		
Stakeholders		
Funding		
Schedule		
Technical Requirements		
Human System Integration		
Criticality of Interfaces		
Seamless Operation		
Information from Comparison Provides Prescriptive Model		
Prescriptive Model for Joint System		
	Integration	Interoperability
Purpose/Capabilities		
Scope of I ²		
Stakeholders		
Funding		
Schedule		
Technical Requirements		
Human System Integration		
Criticality of Interfaces		
Seamless Operation		

Table 4. System of Systems I² Framework

1. Standardized Attributes for Models

Standardized attributes were assigned to each row within the descriptive and normative models of the framework. These choices were selected by the authors based on the findings from research in Chapters III and IV. These attributes were utilized to synthesize both the descriptive model, Table 5, and the normative (notional) model, Table 6. This created a standardized comparison approach to formulate the gap analysis. For clarification, the terminology pertaining to the models is provided below:

As defined by Merriam-Webster, an Enterprise is a business organization (<http://www.merriam-webster.com/dictionary/enterprise>). For example, a large corporation or government agency is an enterprise.

As extracted from the Defense Acquisition Guidebook (2006), a

System of Systems is a set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will significantly degrade the performance or capabilities of the whole. The development of a system of systems solution will involve a trade space between the systems as well as an individual system's performance. For example, the USCG Deepwater program is a system of systems.

A Family of Systems is a grouping of systems having some common characteristic(s). For example, each system in a family of systems may belong to a domain or a product line (e.g., a family of missiles or aircraft). A family of systems lacks the synergy of a system of systems. The family of systems does not acquire qualitatively new properties as a result of the grouping. In fact, the member systems may not be connected into a whole (https://akss.dau.mil/DAG/Guidebook/IG_c4.2.6.asp). For example, the Future Combat System is a family of systems.

A standalone system is one that can operate independently without external support from a functional perspective. For example, a microwave oven qualifies as a standalone system.

Integration: the program addresses integration to make whole or complete by adding or bringing together parts; unify.

Interoperability: the ability of a system or component to function effectively with other systems or components.

	Standardized Attributes for Descriptive Model
Purpose/Capabilities	Well defined, not defined, not addressed, changing, no immediate need
Scope of I2	Enterprise design, SoS, FoS, standalone
Stakeholders	Involved, too Involved, provided strategy, part of decision making at all levels, etc
Funding	Shoe string, well funded, not funded, no stable funding, rolling funding (funds as project progresses)
Schedule	Adequate, rushed, used artificial deadlines, no schedule slip allowed
Technical Requirements	Cutting edge, bleeding edge, unknown, COTS based, partially defined, adequately defined
Human System Integration	Well trained, not well trained, no HSI interface, adequate HSI interface, adequate documentation, unknown documentation, considered critical to the design,
Criticality of Interfaces	Well defined, not fixed, outside of program control
Seamless Operation	Required, Not Required

Table 5. Definitions and Standardized Attributes for Descriptive Table

2. Normative Model (Notional)

The Normative Model was developed as a notional model by reviewing all the positive attributes defined in the standardized descriptive model. The standard phrases were derived from the various programs researched in this thesis.

Normative Model (Notional)		
	Integration	Interoperability
Purpose/Capabilities	Well defined	Well defined
Scope of I2	Enterprise design, SoS, FoS, standalone	Enterprise design, SoS, FoS
Stakeholders	Involved Part of Decision Making Provided Strategy	Involved Part of Decision Making Provided Strategy
Funding	Well Funded Stable	Well Funded Stable
Schedule	Adequate	Adequate
Technical Requirements	Adequately Defined	Adequately Defined
Human System Integration	Considered critical to design	Considered critical to design
Criticality of Interfaces	Well Defined	Well Defined
Seamless Operation	Required	Required


Table 6. Standardized Attributes for Normative Notional Model

C. GAP ANALYSIS USING SYSTEM OF SYSTEMS FRAMEWORK FOR I2

1. Unmanned Air Vehicles Analysis

a. *Unmanned Air Vehicles Descriptive and Normative Model*

The outlined cells in bold in the Descriptive Model reflect the area where a prescription is warranted and will have further explanation in the Prescriptive Model, Table 8.



System of Systems I2 Framework		
Unmanned Air Vehicles		
Descriptive Model		
	Integration	Interoperability
Purpose/Capabilities	Well Defined	Changing
Scope of I2	Standalone	Family of Systems
Stakeholders	Involved	Too little Involvement
Funding	Well Funded	Not Defined
Schedule	Rushed	Rushed
Technical Requirements	COTS Based Cutting Edge	Partially Defined
Human System Integration	Well Trained	Unknown
Criticality of Interfaces	Well Defined	Outside Program Control
Seamless Operation	Required	Initially Not Required Now Required
Compare Descriptive Model Against Normative Model		
Normative Model (Notional)		
	Integration	Interoperability
Purpose/Capabilities	Well Defined	Well Defined
Scope of I2	Enterprise Design, SoS, FoS, Standalone	Enterprise Design, SoS, FoS
Stakeholders	Involved Part of Decision Making Provided Strategy	Involved Part of Decision Making Provided Strategy
Funding	Well Funded Stable	Well Funded Stable
Schedule	Adequate	Adequate
Technical Requirements	Adequately Defined	Adequately Defined
Human System Integration	Considered Critical to Design	Considered Critical to Design
Criticality of Interfaces	Well Defined	Well Defined
Seamless Operation	Required	Required

Table 7. Unmanned Air Vehicles Description and Normative Model

b. Unmanned Air Vehicles Prescriptive Model

The cells with text reflect the initiation of a prescription for this program to support interoperability. Further study is required to develop a full prescription. The blank cells indicate there were not any significant challenges in these areas.

Prescriptive Model for Unmanned Air Vehicles		
	Integration	Interoperability
Purpose/Capabilities		Joint Tactics, Training, and Procedures (TTP) Critical to Concept Design Phase
Scope of I2		
Stakeholders		Involve Operational Reps, Joint Forces Command, and Coalition Partners
Funding		Required
Schedule		Needs to be Established
Technical Requirements		Critical in Concept Design Phase with Trade-offs
Human System Integration		Critical in Concept Design Phase with Trade-offs
Criticality of Interfaces		Critical in Concept Design Phase with Trade-offs
Seamless Operation		Testing in an Operational Environment

Table 8. Unmanned Air Vehicles Prescriptive Model

2. Future Combat System Analysis

a. *Future Combat System Descriptive and Normative Model*

Table 9 displays the FCS Descriptive and Normative Model. Upon review, it is evident a prescription is not necessary at this point in time.

System of Systems I2 Framework		
Future Combat System		
Descriptive Model		
	Integration	Interoperability
Purpose/Capabilities	Well-defined	Well-defined
Scope of I2	Enterprise Design	Enterprise Design
Stakeholders	Involved, Part of decision making	Involved, Part of decision making
Funding	Well Funded	Well Funded
Schedule	Adequate	Adequate
Technical Requirements	Cutting Edge, COTS Based,	Cutting Edge, COTS Based,
Human System Integration	Considered critical to the design	Considered critical to the design
Criticality of Interfaces	Well Defined	Well Defined
Seamless Operation	Required	Required
Compare Descriptive Model Against Normative Model		
Normative Model (Notional)		
	Integration	Interoperability
Purpose/Capabilities	Well defined	Well defined
Scope of I2	Enterprise design, SoS, FoS, standalone	Enterprise design, SoS, FoS
Stakeholders	Involved Part of Decision Making Provided Strategy	Involved Part of Decision Making Provided Strategy
Funding	Well Funded Stable	Well Funded Stable
Schedule	Adequate	Adequate
Technical Requirements	Adequately Defined	Adequately Defined
Human System Integration	Considered critical to design	Considered critical to design
Criticality of Interfaces	Well Defined	Well Defined
Seamless Operation	Required	Required

Table 9. Future Combat System Descriptive and Normative Model

3. Enterprise Joint System Analysis

a. Enterprise Joint System Descriptive and Normative Model

The outlined cells in bold in the Descriptive Model reflect the area that a prescription is warranted and will have further explanation in the Prescriptive Model, Table 10.

System of Systems I2 Framework		
Enterprise Joint System		
Descriptive Model		
	Integration	Interoperability
Purpose/Capabilities	Well-defined	Not addressed No immediate need
Scope of I2	Enterprise	Enterprise
Stakeholders	Management No end-users	Management No end-users
Funding	Stable Funding	None
Schedule	Adequate	None
Technical Requirements	Well-defined	Not defined
Human System Integration	Not defined	Not defined
Criticality of Interfaces	Well-defined	Not defined
Seamless Operation	Required	Not required
Compare Descriptive Model Against Normative Model		
Normative Model (Notional)		
	Integration	Interoperability
Purpose/Capabilities	Well defined	Well defined
Scope of I2	Enterprise design, SoS, FoS, standalone	Enterprise design, SoS, FoS
Stakeholders	Involved Part of Decision Making Provided Strategy	Involved Part of Decision Making Provided Strategy
Funding	Well Funded Stable	Well Funded Stable
Schedule	Adequate	Adequate
Technical Requirements	Adequately Defined	Adequately Defined
Human System Integration	Considered critical to design	Considered critical to design
Criticality of Interfaces	Well Defined	Well Defined
Seamless Operation	Required	Required

Table 10. Enterprise Joint System Descriptive and Normative Model

b. Enterprise Joint System Prescriptive Model

The cells with text reflect the initiation of a prescription for this program to support interoperability and augment integration. Further study is required to develop a full prescription. The blank cells indicate there were not any significant challenges in these areas.

Prescriptive Model for Joint System		
	Integration	Interoperability
Purpose/Capabilities		Provide vision to anticipate need
Scope of I2		
Stakeholders	Involve end-users	Involve end-users
Funding		Inclusive
Schedule		Inclusive
Technical Requirements		Critical in Concept Design Phase
Human System Integration	Critical in Concept Design Phase	Critical in Concept Design Phase
Criticality of Interfaces		Critical in Concept Design Phase
Seamless Operation		

Table 11. Enterprise Joint System Prescriptive Model

D. SUMMARY

Based on the gap analysis, it is critical and vital to initiate I² investigation prior to the concept design phase of the product development lifecycle in order to produce systems that are interoperable and that ensure integration.

The authors contend that conducting a systems integration process, through an I² Analysis, provides assurance to the customer that all system elements will function as a whole. Systems integration extends to the holistic notion that involves all of the organizational components of an enterprise during the entire cycle of the acquisition process and needs to begin during stakeholder analysis.

1. I² Analysis

According to Langford, Franck, Huynh & Lewis, 2007, the purpose of the Stakeholder Analysis is to provide a process of a systematic method of identifying the stakeholders and their needs, value and interests. This initial brainstorming and discussion period among stakeholders is a critical point to initiate dialogue and gather

data points to ensure I^2 capabilities such as complexity of the system of systems, required critical functions, and potential risks. This sets the stage for the design and development of the I^2 Analysis, which needs to be continued throughout the product development lifecycle (Blanchard & Fabrycky, 2006).

The I^2 Analysis needs to be a continuous thread across the product development lifecycle. Figure 6 is an adaptation from (Blanchard & Fabrycky, Figure 12.2, 2006) which overlays an I^2 Analysis structure to introduce the concept of recognizing I^2 Analysis as a standard systems engineering approach that needs to be addressed through all the considerations such as requirements, architecture, risk analysis, cost estimation, testing, evaluation, and maintenance.

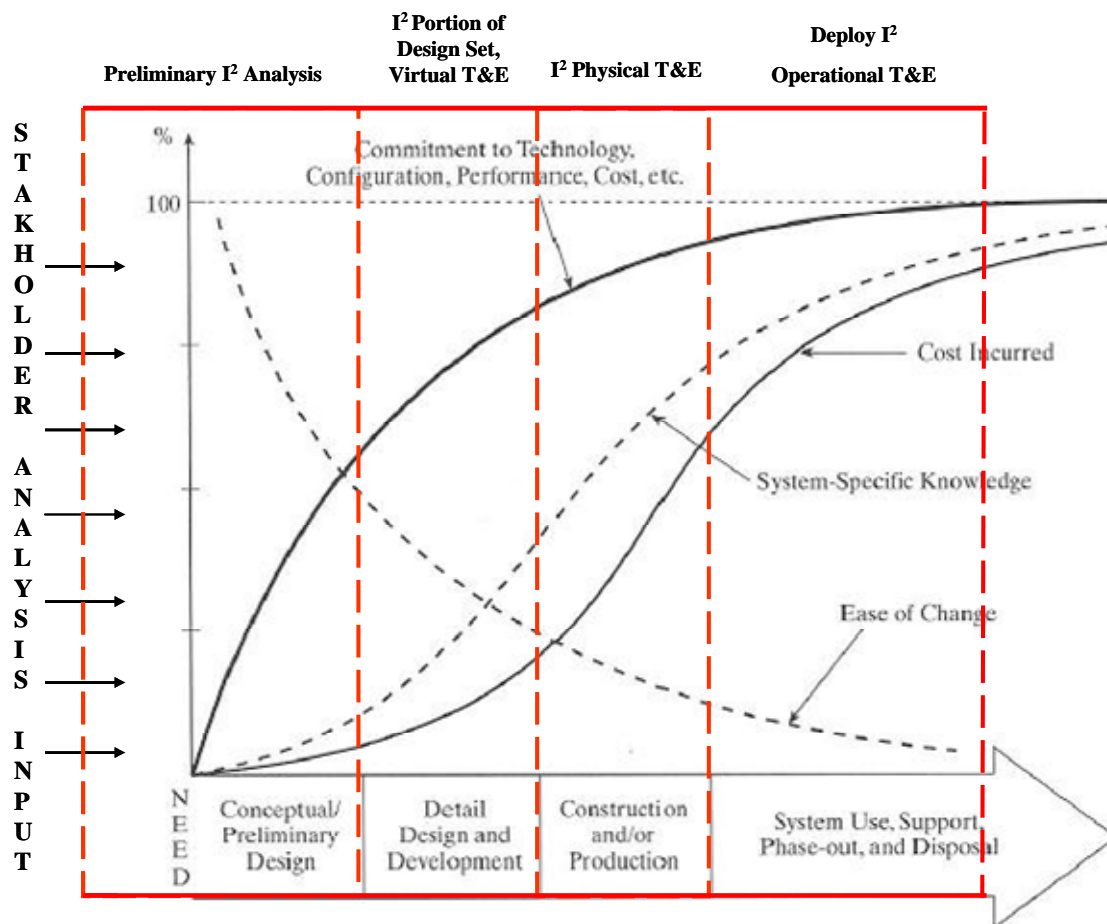


Figure 6. I^2 Analysis Stages.

As shown by the I^2 references in Figure 6, which augments the original (Blanchard & Fabrycky, Figure 12.2, 2006), the authors of this thesis introduce I^2 Analysis as a new procedure or technique recommended in the system engineering framework to support interoperability and ensure integration of system of systems. The key is to initiate the analysis at the stakeholder analysis phase to receive input that is incorporated into the needs assessment and continued throughout the product development lifecycle through various stages such as:

- Preliminary I^2 Analysis, I^2 Portion of Design Set, Virtual T&E (modeling and simulation), I^2 Physical T&E, and Deploy Operational T&E.
- Further research and development needs to be conducted to develop this concept and the stages of I^2 .

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. KEY RESEARCH FINDINGS

This chapter answers the research questions posed by the authors in Chapter I. The lessons learned section in this chapter will expound upon the four key attributes related successful I² systems below.

1. Common and known Operational Environment
2. Governance of the I² boundaries
3. I² based acquisition, not schedule or funding
4. Early Establishment of I² requirements

In Chapter V, I² was introduced as a new procedure; below are some granular level techniques and procedures that also are recommended:

- Improve capability architecting
- Utilize modeling and simulation
- Perform operational assessments during development test

B. LESSONS LEARNED

1. How do the Current Policies and Processes of Successful Large System of Systems Designs Support I²?

Based on the research in this thesis, there are over eighty-eight statutory laws, regulatory laws, and various DoD instructions that address the requirement/need to develop systems that are I². Chapter II has outlined many of these policies and processes.

No doubt, the current policies and processes assisted in defining the system designs to attempt I² but as outlined in Chapter IV, prematurely declare victory. It is insufficient to claim that all I² capabilities have been met because the design passes the open standards test and evaluation. The policies related to I² are meaningless unless the leadership (i.e., Program Manager, Chief System Engineering) strictly enforce these policies and procedures. These I² policies and processes that are not clearly defined allow for misinterpretation and misuse. Specifically, missing from policies and processes is the quantitative definition of what constitutes an integrated and interoperable system.

The successful large systems described in Chapter IV seemed to address I² up front and early in the system design. These programs addressed not only well defined requirements in most cases but also extensive testing during development to ensure I² capabilities. For example, with the FCS, the program established an entire Brigade in Arizona for full-time large scale operational testing to ensure I² capabilities.

For other programs that deal with I² as just another requirement, without clearly defined policies and processes related to I², and with limited compliance checking or any checks-and-balances, this issue of systems being fielded that are not I² will most certainly continue. A program needs to ensure that prioritization and program funding is aligned to address I² as part of the acquisition process. In addition, from this research it is worth noting that successful programs have shown responsibility and governance across the entire system of systems or enterprise and I² is central to achieving the fielded capabilities.

2. How Effective are the Existing Laws and DoD Instructions in ensuring Integration and Interoperability?

Based on the various systems investigated in this thesis, successful I² depends on the system design practices and ultimately the program office or service to allocate schedule and funding for the activity in the concept design phase, which includes capability analysis and functional decomposition. The existing laws and instructions assume programs allocate sufficient resources for this level of system engineering.

As described in Chapter II, findings from GAO and others point to priority issues for an acquisition team that are created by DoD and Congress to ensure funding is spent, milestones are achieved, and the following year's increment of funding is not lost. The real focus of these laws has not been on I² of systems. Consequently, these laws state the needs to be I² but never attempt to describe and quantify this characteristic. Based on a historical perspective, most of the I² laws and follow-on instructions were written to address past program failures; however, but until the debate is finished regarding quantified terms for I², history is sure to repeat.

These laws and instructions are only as effective as the oversight, planning, and execution of the system engineering principles – which begin with good system requirements. Currently, our research shows there is limited schedule and funding to truly follow these laws and instructions. Only in conjunction with a system's Initial Operational Capability is there funding and schedule identified to patch the I² challenges once a system is fielded.

3. What are the Key Attributes that Result in an I2 System?

Integration and interoperability within the context of this thesis has been primarily focused on vehicles (i.e., Space Shuttle), weapons (i.e., FCS), and sensors (i.e., UAV). How these systems are integrated and their degree of interoperability has been summarized in the Descriptive Framework in Chapter V. Reviewing the programs described in this thesis, there are a few common themes that support I2 development of systems.

Observations common across many of the programs include the following.

a. Common and Known Operational Environment

For system capabilities that are developed by multiple program offices, there needs to be a common operational environment (i.e., ground combat, humanitarian support) to be defined and coordination among the systems.

The Combat ID or UAV programs described in Chapters III and IV are examples of DoD programs in which all services have systems either fielded or being developed with minimal coordination beyond standard interfaces. The Joint operational environment for Combat ID or UAVs would be the starting point for a systems engineering decomposition to system activities and further allocation to system functions would continue through to the critical I² points necessary for these multiple systems.

These operational environments need to be agreed upon by all services and tested during an individual system's developments and during any number of the Joint integration exercises that are conducted yearly. It requires the program managers and system engineers to plan, coordinate, and prepare for these events.

b. Governance of the I² Boundaries

An I² boundary is the external interface between one system and another system. This external interface can be architected as a peer-to-peer, system of systems, or net-centric topology. An I² defined boundary is more than just protocols or addressing. An I² boundary includes specific data structures, common data units, timeliness, and quality of data as well as standard data and transmission protocols.

The capabilities developed within tightly integrated systems with seamless integration must be deliberately engineered. The timeliness, quantity, and quality of the information that is critical and relevant to the overall capability can be difficult to define.

Programs like FCS and the Space Shuttle are system of systems that are also well integrated and interoperable. These programs have structured systems engineering processes in place that include configuration management within and across the various systems and subsystems. These successful programs also feature governance over the I² boundaries.

The I² across federated systems that are not within a single acquisition authority structure spreads Program Manager Title 10 authority across multiple systems. The United States Code (USC) Title 10 gives the Armed Forces various discrete statutory authorities. Various public laws defined in Chapter II have added detail or scope to this section of USC. A Program Manager with Title 10 authority has overall responsibility for all aspects of the program and no other individual can change, direct, or modify the Program Manager's decision. Provided programs work together initially and develop those critical I² interfaces there is not a single external authority capable of ensuring that the I² boundary configuration remains constant.

From a system of systems or Net-Centric perspective, such programs have explicit or imexplicit I² requirements. Persistent system engineering analyses across these individual programs can refine and establish the necessary requirement to ensure an I² capability. The limited authority to require program managers to adjust and correct I² issues is met with significant resistance and Title 10 authority that seems to supersede the DoD or Congress's mandate for of I².

c. I² Based Acquisition, Not Schedule or Funding

A common theme across programs that have been unsuccessful to attain I² completely is the lack of schedule or funding necessary to develop I² solutions.

Programs like Deepwater may have had adequate funding but based on contracted deliverables had tight schedule with little room for error. As many GAO reports referenced in this thesis have pointed out, program managers are focused on schedules and securing funding or keeping funding.

Many well-developed I² systems in operations today did not initially deploy as such. Most of these systems traded off I² and performance to meet schedule or cost realities.

A recommended follow-on thesis could be the establishment of a framework for performance and I² based acquisition.

d. Early Establishment of I² Requirements

As part of the programs reviewed in this thesis, the systems that had well-implemented I² had either I² requirements developed early in the design or as a part of a spiral acquisition strategy, with scheduled and funded demonstrations and user evaluations and demonstrations.

An example of this is the FCS program. From a capability definition, the FCS actively exchanges data between systems and across the family of systems design. Early in design, the FCS program had specific requirements to be interoperable via a net-centric, tightly integrated architecture. These requirements were further decomposed which resulted in a Service Oriented Architecture (SOA) as the framework of FCS.

To ensure I² requirements and the proposed implementation are correct, FCS has scheduled and funded I² into the program operational assessments with not only Army operators but also joint tests with other ground combat units to include the Marine Corps. The result of these tests identified various problems in the implementation of some requirements and FCS corrected these issues as part of their open development testing events.

4. What New Recommendations Can Support Interoperability and Ensure Integration of System of Systems?

The overall complexity of the systems design and type of architecture selected to achieve the required capability has a relationship to the amount of system engineering necessary to support interoperability and ensure integration.

The following are some recommendation:

a. Improve Capability Architecting

Capability based acquisition depends upon fielding I² systems to the operators that delivers the required capability. An example of this is the Army's Improvised Explosive Device (IED) jammer. The development and fielding of the Army's IED jammer was successful in blocking IED detonation signals. However, initial deployment of these units also jammed all platform communications. A jammer was fielded but the capability to jam IED signals while performing warfighting missions was not.

Similar to system integration, capability integration is needed. As new requirements for new capabilities are established, the integration of these new requirements into the large warfighting functions need to be analyzed to identify I² risk areas.

Requirements that are decomposed from capability documents (i.e. JCIDS CCD and CPD) should include potential I² issues with other capabilities either already fielded or currently in design in order to alert the program office and there engineering staff.

b. Modeling and Simulation

Modeling and Simulation (M&S) has been used for many programs to address mechanical issues, evaluate physical problems of a design, investigate critical timing issues, etc. Depending on the program, M&S was necessary to reduce risk or evaluate designs before production.

M&S on I²-focused events is not prevalent in the literature. This type of M&S is more about the development of the Interface Control Documents of a program via M&S evaluation. This upfront systems engineering could ensure I² early in the lifecycle of a program.

c. Operational Assessments during Development Test

It will be many years, if ever, before completely-accurate I² requirements are established for new acquisition programs. This is not a trivial endeavor. Requirements vetted through any of the current acquisition processes still are not adequate to ensure the design is I².

Operational assessments during the requirements allocation phase could be the point in which the end users get engaged in the design process. These early operational assessments would be a crucial review of the I² aspect of the systems. A similar review may also be conducted when any I² requirements need to be established with other systems and capabilities that are already in use.

Operational assessments during the early design phases should be conducted with simulators or real systems with which the new system is to be I². These types of assessments in the form of lab tests should be conducted multiple times during the development and should be critical during Independent Verification and Validation IV&V testing.

C. FUTURE RESEARCH

The following are potential topics for future research in developing techniques for more integrated and interoperable system of systems:

- Develop quantitative metrics corresponding to each cell of the Normative Model. These would logically have stakeholder weightings as input.
- Investigate more examples from other industries (e.g., medical) with the quantitative metrics mentioned above applied to solidify the findings of this study.
- Investigate how one would address the "devil-in-the-detail" details that are the ultimate problems with getting system of systems to be integrated and interoperable since this thesis addresses these issues at a very high-level.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. STATUTORY LAWS

A. PUBLIC LAW 104-106-FEB. 10, 1996

1. According to Public Law 104-106-Feb. 10, 1996:

INTEGRATION

DIVISION A-DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE 1-PROCUREMENT

Subtitle B-Program Requirements, Restrictions, and Limitations

SEC. 225. ADVANCED FIELD ARTILLERY SYSTEM (CRUSADER).

(a) AUTHORITY TO USE FUNDS FOR ALTERNATIVE PROPELLANT TECHNOLOGIES. – During fiscal year 1996, the Secretary of the Army may use funds appropriate for the liquid propellant portion of the Advanced Field Artillery System (Crusader) program for fiscal year 1996 for alternative propellant technologies and integration of those technologies into the design of the Crusader.

...(6) Development, for integration into the next prototype of the cannon, of engineering designs to control pressure oscillations in the chamber of the cannon during firing...

Summary: Integration of present cannon system characteristics to control specific operability issues, i.e., chamber pressure oscillations.

Subtitle C-Ballistic Missile Defense Act of 1995

SEC. 234. THEATER MISSILE DEFENSE ARCHITECTURE.

...(c) INTEROPERABILITY AND SUPPORT OF CORE SYSTEMS. - To maximize effectiveness and flexibility of the systems comprising the core theater missile defense program, the Secretary of Defense shall ensure that systems are integrated and complementary and are fully capable of exploiting external sensor and battle management support from systems such as –

- (A) the Cooperative Engagement Capability (CEC) system of the Navy;
- (B) airborne sensors; and
- (C) space-based sensors (including, in particular, the Space and Missile Tracking System.)...

Summary: Core missile systems must be fully interoperability with other DoD systems.

Subtitle E – Miscellaneous Reviews, Studies, and Reports

SEC. 261. PRECISION-GUIDED MUNITIONS.

(a) ANALYSIS REQUIRED. – The Secretary of Defense shall perform an analysis of the full range of precision-guided munitions in production and in research, development, test, and evaluation in order to determine the following:

(1) The numbers and types of precision-guided munitions that are needed to provide complementary capabilities against each target class.

(2) The feasibility of carrying out joint development and procurement of additional types of munitions by more than one of the Armed Forces.

(3) The feasibility of integrating a particular precision-guided munition on multiple service platforms...

Summary: Precision guided munitions must be interoperable with multiple platforms.

INTEROPERABILITY

SEC. 262. REVIEW OF C4I BY NATIONAL RESEARCH COUNCIL.

...(b) MATTERS TO BE ASSESSED IN REVIEW. – The review shall address the following:

(1) The match between the capabilities provided by current service and defense-wide C4I programs and the actual needs of users of these programs.

(2) The interoperability of service and defense-wide C4I systems that are planned to be operational in the future.

(3) The need for an overall defense-wide architecture for C4I.

(4) Proposed strategies for ensuring that future C4I acquisitions are compatible and interoperable with an overall architecture...

Summary: Gap analysis to ensure C4I needs are met for all DoD systems.

TITLE LIII – INFORMATION TECHNOLOGY ACQUISITION PILOT PROGRAMS

Subtitle A – Conduct of Pilot Programs

SEC. 5312. SOLUTIONS-BASED CONTRACTING PILOT PROGRAM.

...(C) PROCESS REQUIREMENTS. – The Administrator shall require use of a process with the following aspects for acquisitions under the pilot program:...

...(d) PILOT PROGRAM DESIGN...

...(3) COMPLEXITY OF PROJECTS...

...(B) In order for an acquisition project to satisfy the requirement in subparagraph (A), the solution for attainment of the executive agency's objectives under the project should not be obvious, but rather shall involve a need for some innovative development and systems integration...

Summary: Role and necessity of systems integration in information technology acquisition programs.

B. PUBLIC LAW 105-261-OCT. 17, 1998

1. According to Public Law 105-261-Oct. 17, 1998:

INTEGRATION

DIVISION A – DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE XV – MATTERS RELATING TO ARMS CONTROL, EXPORT CONTROLS, AND COUNTERPROLIFERATION

Subtitle B – Satellite Export Controls

SEC. 1514. NATIONAL SECURITY CONTROLS ON SATELLITE EXPORT LICENSING.

(B) CONTENTS OF MONITORING. – The monitoring under subparagraph (A) shall cover, but not be limited to-

...(ii) satellite processing and launch activities, including launch preparation, satellite transportation, integration of the satellite with the launch vehicle, testing and checkout prior to launch, satellite launch, and return of equipment to the United States:..

Summary: System integration specifics must be export controlled in addition to system design and operational details.

INTEROPERABILITY

TITLE III – OPERATION AND MAINTENANCE

Subtitle D – Information Technology Issues

SEC. 331. ADDITIONAL INFORMATION TECHNOLOGY RESPONSIBILITIES OF CHIEF INFORMATION OFFICERS.

...(2) ensure the interoperability of information technology and national security systems throughout the Department of Defense;...

Summary: Interoperability is essential among different computer based systems in the DoD.

SEC. 335. CONTINUITY OF ESSENTIAL OPERATIONS AT RISK OF FAILURE BECAUSE OF INFORMATION TECHNOLOGY AND NATIONAL SECURITY SYSTEMS THAT ARE NOT YEAR 2000 COMPLIANT.

...(b) CONTENT. The report shall contain, at a minimum, the following:...

...(7) A discussion of the vulnerability of allied armed forces to the failure of systems that are not, or have critical components that are not, year 2000 compliant,

together with an assessment of the potential problems for interoperability among the Armed Forces of the United States and allied armed forces because of the potential for failure of such systems...

Summary: The impact of Y2K compliance on the interoperability of military systems.

Subtitle E – Defense Infrastructure Support Improvement

SEC. 344. OVERSIGHT OF DEVELOPMENT AND IMPLEMENTATION OF AUTOMATED IDENTIFICATION TECHNOLOGY.

...(3) As part of its oversight responsibilities, the Automated Identification Technology Office shall establish standards designed –

(A) to ensure the compatibility and interoperability of automated identification technology programs in the Department of Defense; and ...

Summary: Interoperability is essential for DoD automated identification technologies.

TITLE IX – DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

Subtitle C – Joint Warfighting Experimentation

SEC. 922. SENSE OF CONGRESS CONCERNING JOINT WARFIGHTING EXPERIMENTATION.

...(b) Resources and Authority of Commander...

...(5) Providing the Secretary of Defense and the Chairman of the Joint Chiefs of Staff with recommendations, based on the conduct of joint warfighting experimentation, for –

improving interoperability;

reducing unnecessary redundancy;

synchronizing technology fielding;

developing joint operational concepts;

prioritizing the most promising joint capabilities for future experimentation; and

prioritizing joint requirements and acquisition programs...

Summary: Recommendations for interoperability improvements in joint warfighting capabilities.

TITLE XII – MATTERS RELATING TO OTHER NATIONS

Subtitle C – Matters Relating to NATO and Europe

SEC. 1222. REPORT ON MILITARY CAPABILITIES OF AN EXPANDED NATO ALLIANCE.

...(1) An assessment of the tactical, operational, and strategic military requirements, including interoperability, reinforcement, and force modernization issues, as well as strategic and territorial issues, that are raised by the inclusion of Poland, the Czech Republic, and Hungary in the NATO alliance...

Summary: Interoperability issues concerning the expanded NATO alliance.

C. PUBLIC LAW 107-314-DEC. 2, 2002

1. According to Public Law 107-314-Dec. 2, 2002:

INTEGRATION

DIVISION A-DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE X – GENERAL PROVISIONS

Subtitle B – Naval Vessels and Shipyards

SEC. 1025. SHIP COMBAT SYSTEM INDUSTRIAL BASE.

(A) REVIEW. – The Secretary of Defense shall conduct a review of the effect of the contract award announced on April 29, 2002, for the lead design agent for the DD(X) ship program on the industrial base for ship combat system development, including the industrial base for each of the following: ship systems integration, radar, electronic warfare, and launch systems.

Summary: Review the impact of DD(X) contract award on ship systems integration.

INTEGRATION AND INTEROPERABILITY

Subtitle C – Strategic Matters

SEC. 1032. ANNUAL REPORT ON WEAPONS TO DEFEAT HARDENED AND DEEPLY BURIED TARGETS.

(b) REPORT ELEMENTS. – The report for a fiscal year under subsection (a) shall –

(1) include a discussion of the integration and interoperability of the activities referred to in that subsection that were undertaken during that fiscal year, including a discussion of the relevance of such activities to applicable recommendations by the Chairman of the Joint Chiefs of Staff...

Summary: Integration and interoperability of “Bunker Buster” systems which is conventional bomb used to destroy deeply buried targets.

TITLE XII – MATTERS RELATING TO OTHER NATIONS

SEC. 1205. COMPREHENSIVE ANNUAL REPORT TO CONGRESS ON COORDINATION AND INTEGRATION OF ALL UNITED STATES NONPROLIFERATION ACTIVITIES.

...(d) ANNUAL REPORT ON IMPLEMENTATION OF PLAN...

“(C) a discussion of cooperation, coordination, and integration during such year in the implementation of the plan among the various departments and agencies of the United States Government, as well as private entities that share objectives similar to the objectives of the plan; and...

Summary: Reviews integration issues related to weapons nonproliferation activities of various DoD related organizations.

INTEROPERABILITY

TITLE XIII – OPERATIONS AND MAINTENANCE

Subtitle F – Information Technology

SEC. 353. INSTALLATION AND CONNECTION POLICY AND
PROCEDURES REGARDING DEFENSE SWITCH
NETWORK..

...(b) ELEMENTS OF POLICY AND PROCEDURES.- The policy and procedures shall address at a minimum the following:

(1) Clear interoperability and compatibility requirements for procuring, certifying, installing, and connecting telecom switches to the Defense Switch Network.

(2) Current, complete, and enforceable testing, validation, and certification procedures needed to ensure the interoperability and compatibility requirements are satisfied...

...(d) INVENTORY OF DEFENSE SWITCH NETWORK.- The Secretary of Defense shall prepare and maintain an inventory of all telecom switches that, as of the date on which the Secretary issues the policy and procedures-

(1) are installed or connected to the Defense Switch Network; but

(2) have not been tested, validated, and certified by the Defense Information Systems Agency (Joint Interoperability Test Center).

(e) INTEROPERABILITY RISKS. – On an ongoing basis, the Secretary of Defense shall –

(1) identify and assess the interoperability risks that are associated with the installation or connection of uncertified switches to the Defense Switch Network and the maintenance of such switches on the Defense Switch Network; and

(2) develop and implement a plan to eliminate or mitigate such risks as identified...

Summary: Interoperability issues, i.e., risks, etc. with connecting civilian telecommunication switches to the defense switch network.

TITLE VII – HEALTH CARE PROVISIONS

Subtitle C – Department of Defense-Department of Veterans Affairs
Health Resources Sharing

SEC. 724. INTEROPERABILITY OF DEPARTMENT OF VETERANS AFFAIRS AND DEPARTMENT OF DEFENSE PHARMACY DATA SYSTEMS.

(a) INTEROPERABILITY. – The Secretary of Veterans Affairs and the Secretary of Defense shall seek to ensure that on or before October 1, 2004, the Department of Veterans Affairs pharmacy data system and the Department of Defense pharmacy data system (known as the “Pharmacy Data Transaction System”) are interoperable for both Department of Defense beneficiaries and Department of Veterans Affairs beneficiaries by achieving real-time interface, data exchange, and checking of prescription drug data of out-patients, and using national standards for the exchange of out-patient medication information...

Summary: Mandate interoperability of DoD and Veterans Administration pharmaceutical information gathering for veterans receiving medication.

Subtitle A – Acquisition Policy and Management

TITLE VIII – ACQUISITION POLICY, ACQUISITION MANAGEMENT, AND RELATED MATTERS

SEC. 802. REPORT TO CONGRESS ON EVOLUTIONARY ACQUISITION OF MAJOR DEFENSE ACQUISITION PROGRAMS

...(b) CONTENT OF REPORT. – The report shall, at a minimum, address the following matters:...

...(3) The manner in which the Secretary plans to ensure that each increment of an evolutionary acquisition process is designed-

(A) to achieve interoperability within and among United States forces and United States coalition partners; and...

Summary: Defense acquisition programs need to incorporate interoperability requirements.

The statutory laws are to ensure Institutions, Commands, Program Managers, and individuals are held liable for their actions or lack of action related to the I² systems. Congress enacted these laws but imposed minimal criminal penalties to ensure integration or interoperability while performing business related duties. This situation imposes a general duty on Program Managers or Commands but does not identify criminal sanctions against an individual who fails to meet the I² requirements.

APPENDIX B. REGULATORY LAWS

A. JOINT PUBLICATION 1

According to Joint Publication 1:

The *Doctrine for the Armed Forces of the United States*, May 14, 2007, is the capstone publication for all joint doctrine, presenting fundamental principles and overarching guidance for the employment of the Armed Forces of the United States. In essence, the purpose of this document is to enhance the operational effectiveness of US Forces. An analysis and synthesis of the Joint Publication 1 doctrine follows. (Preface, i).

INTEGRATION

As written in the executive summary,

the National strategic direction is governed by the Constitution, federal law, USG policy regarding internationally-recognized law and the national interest. This direction leads to unified action which is a broad term referring to the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve a unified effort. Xi

At a high level, Chapter III describes

one of the functions and responsibilities within the Department of Defense which is the Integration of the Armed Forces into an effective and efficient team operating within the air, land, maritime, and space domains and the information environment. III-2

This Joint Publication also presents guidelines for interagency coordination

to assure that all participating agencies under appropriate authority focus their efforts on national objectives, specifically the Armed Forces of the United States have unique capabilities to offer the interagency community. These include influence through established military-to-military domestic and international contacts, resources (i.e., logistics) not available to nonmilitary agencies, trained civil affairs personnel and their assets; responsiveness based on military training and readiness. Additional unique military capabilities include C2 resources supported by worldwide communications and ISR infrastructures, robust organizational and planning processes, training support for large numbers of individuals on a myriad skills, and air, land, and sea mobility support for intertheater or intratheater requirements. VII-4

INTEROPERABILITY

As with the Integration section above, unified action also demands maximum interoperability to achieve national strategic direction.

The forces, units, and systems of all Services must operate together effectively. This effectiveness is achieved in part through interoperability. This includes the development and use of joint doctrine, the development and use of joint operation plans; and the development and use of joint and/or interoperable communications and information systems. It also includes conducting joint training and exercises. Xii

In chapter I, Foundations, the fundamentals highlight the Joint Force.

Twenty years after the Goldwater-Nichols Department of Defense (DoD) Reorganization Act (Title 10, US Code [USC], Sections 151-155) directed actions to remove the institutional barriers to jointness, the Armed Forces of the United States is a joint team. All Service components contribute their distinct capabilities to the joint campaign; however, their interdependence is critical to overall joint effectiveness. Joint interdependence is the purposeful reliance by one Service on another Service's capabilities to maximize complementary and reinforcing effects of both; the degree of interdependence varying with specific circumstances. Fundamentally, joint forces require high levels of interoperability and systems that are "born joint" (i.e., conceptualized and designed with joint architectures and acquisition strategies). This level of interoperability ensures that technical, doctrinal, and cultural barriers do not limit the ability of Joint Force Commanders to achieve objectives. The goal is to design joint force capabilities – lethal and nonlethal – to fight and win the Nation's wars and effectively carry out all other missions assigned across the range of military operations. I-2

In Chapter II,

Doctrine Governing Unified Direction of Armed Forces, under the section Relationship Between Combatant Commanders, Military Secretaries, Service Chiefs, and Forces, highlights interoperability and dictates how unified action demands maximum interoperability. Similar to Chapter 1, the essence is that the forces, units, and systems of all Services must operate together effectively. This effectiveness is achieved in part through interoperability. This includes the development and use of joint doctrine, the development and use of joint operation plans; and the development and use of joint and/or interoperable communications and information systems. It also includes conducting joint training and exercises. It concludes with a materiel development and fielding process that provides

materiel that is fully compatible with and complementary to systems of all Services. A key to successful interoperability is to ensure that planning processes are joint from their inception. Those responsible for systems and programs intended for joint use will establish working groups that fully represent the services and functions that will be affected and interoperability must be considered in all joint program reviews. Combatant Commanders will ensure maximum interoperability and identify interoperability issues to the Chairman of the Joint Chiefs of Staff, who has overall responsibility for the joint interoperability program. **II-7**

In addition, the tenet Organization for Joint Command and Control outlines that

component and supporting commands' organizations and capabilities must be integrated into a joint organization that enables effective and efficient joint C2. The C2 structure is centered on the Joint Force Commander's mission and concept of operations; available forces and capabilities; and joint force staff composition, capabilities, location, and facilities. The Joint Force Commander should be guided in this effort by four principles one of which is interoperability. C2 capabilities within joint force headquarters, component commands, and other supporting commands must be interoperable to facilitate control of forces. The simplest and most streamlined chain of command can be **thwarted by an absence of interoperability** among the components' forces and systems. This includes an emphasis on the use of joint doctrine development of ISR, communications systems, and logistic architectures; joint training and exercises. IV-19

Chapter V, Doctrine for Joint Commands, provides guidance to establish unified and subordinate joint commands.

In regards to interoperability, there are principles to establish a Communications System Directorate of a Joint Staff (J-6). The J-6 assists the Commander in all responsibilities for communications infrastructure, communications computer networking, communications electronics, information assurance, tactical communications, and interoperability. This includes development and integration of communications system architectures and plans that support the command's operational and strategic requirements, as well as policy and guidance for implementation and integration of interoperable communications systems in execution of the mission. V-16

B. JOINT PUBLICATION 6

According to Joint Publications 6:

The *Joint Communications System*, March 20, 2006, contains approved doctrine for communications system support to joint and multinational operations and outlines the responsibilities of Services, agencies, and combatant commands with respect to ensuring effective communications system support to commanders. It addresses how the communications system, in general, is to be configured, deployed, and employed to support the commanders of joint forces in the conduct of joint operations. (Preface, i)

An analysis and synthesis of the Joint Publication 6 doctrine follows.

INTEGRATION

From the Executive Summary, Commander's Overview it states

“Effective command and control (C2) is necessary for proper integration and employment of operational capabilities.” Vii

The objective of the joint communications system is to assist the joint force commander (JFC) in command and control (C2) of military operations. The first element of C2 system is **people** — people who acquire information, make decisions, take action, communicate, and collaborate with one another to accomplish a common goal. The second element of the C2 system taken collectively are the **facilities, equipment, communications, and procedures** essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned. Although families of hardware are often referred to as “systems,” the C2 system is more than simply equipment. High-quality equipment and advanced technology do not guarantee effective C2. Effective C2 starts with well-trained and qualified people and an effective guiding philosophy and procedures. Vii

The power of superiority in the information environment mandates that the United States fight for it as a first priority even before hostilities begin. This requires DoD to develop doctrine, tactics, techniques, and procedures, organizational relationships, and technologies to win this fight. The quality of information depends upon the accuracy, timeliness, relevance, usability, and completeness of information from all sources. A priority responsibility of command is to ensure access to all relevant information sources within and among all DoD and non-DoD organizations, and in multinational operations with mission partners. The continuous sharing of information from a variety of sources facilitates enabling the fully networked joint force to achieve shared situational awareness. I-6

This segment from Chapter I also relates to the Joint Publication 1 segment of this thesis, regarding **Joint Communications System Roles and Responsibilities**. This portion states the

Joint Staff J-6 provides advice and recommendations about communications system matters to the Chairman of the Joint Chiefs of Staff (CJCS). In accordance with Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 8010.01A, Joint Community Chief Information Officer, the J-6 also serves as the joint community Chief Information Officer (CIO). As chairman of the Military Communications-Electronics Board (MCEB), the Director, J-6 utilizes the MCEB to coordinate and resolve Global Information Grid issues among the Services and member agencies. With respect to joint force support, under CJCS authority and direction, and subject to the supervision and guidance of the Director, Joint Staff (DJS), the Director, J-6 normally has the responsibility to: Information Integration (ASD(NII)), ensure that life-cycle management of joint C2 systems has the capability to support the President, the Office of the Secretary of Defense (OSD), Joint Staff, Services, combatant commands, DoD agencies, and any other entity that may comprise a joint operation. I-12

INTEROPERABILITY

Commander United States Strategic Command has overall responsibility for global network operations (GNO) and defense in coordination with the Chairman of the Joint Chiefs of Staff (CJCS) and the other combatant commands. Because the GIG represents the entire communications system of Department of Defense, there remain many decisions regarding planning and design that fall under the purview of the Assistant Secretary of Defense (Networks and Information Integration (ASD [NII])), who is also designated DoD's chief information officer (CIO). Many of those decisions involve the insertion of new technology as well as other architectural standards, which may impact the interoperability of the DoD as a whole. Ix

The hierarchical organization of management impacts the interoperability but as well uniform configuration management of the GIG ensures interoperability and survivability of the DoD information infrastructure. In addition to the expected adherence to DoD policy, GIG configuration is controlled through compliance with the GIG architecture. GIG assets, to include those that are commercial off-the-shelf, are to be configured in accordance with approved capabilities documents and standards and compliant with the operational, system, and technical views of the GIG

architecture. DoD has created various forums to assist the Chief Information Officer, as well as the Chairman and Joint Chiefs of Staff, in compliance determination.

The DoD CIO (ASD [NII]) is responsible for developing, maintaining, and enforcing compliance with the GIG architecture. Inherent in the Chief Information Officer's architecture responsibility is to enforce interoperability, information assurance (IA) net-centric data sharing, use of enterprise services, and GIG program synchronization. II-14

In Chapter III, the Joint Force Communications System Operations Planning and Management Structure outlines

...the CCDR, through the J-6, provides communications system guidance and priorities to supporting commands and components. The J-6 is responsible to the Joint Force Commander for providing the communications system to support reliable, timely information flow in support of unified action. The J-6 assists the Joint Force Commander in all communications systems responsibilities. III-1

Within Chapter III is also the communication planning and management section that details a methodology for communication system planning into five areas: mission analysis, information needs analysis, interoperability, compatibility, and supportability analysis, capability analysis, and allocation of communications system assets.

(1) **Mission Analysis.** During mission analysis, communications system planners develop the communications system estimate and specified and implied tasks to be performed by operators and communications system personnel. The communications system estimate is the J-6's assessment of course of actions that serve as the foundation of the commander's estimate, mission statement, intent, commander's critical information requirements (CCIRs), and concept of operations and support of it. Using foundational knowledge of the C2 organization and communications system capabilities, planners translate the concept of operations, concept of support, CCIRs, and environment into specified and implied tasks during each phase of operations. Tasks are developed for the deployment, implementation, operations, sustainment, modification and restoration of C2 systems and networks to achieve IS throughout operations and support. Network management tools and C2 systems facilitate planning as well as SA.

(2) **Information Needs Analysis.** Communications system planners work closely with all functional communities to develop information exchange requirements (IER). IERs identify products to be transmitted and received,

as well as the throughput, quantity, and characteristics of those products. The communications system is tailored to meet the projected IERs. During military operations, planners conduct analysis to see if the mission, concept of the operation and support, CCIRs and C2 organization necessitate the increase or decrease of the IERs, or new exchange requirements. Adjustments are made to the IERs as appropriate. *For a more detailed discussion of IERs, refer to CJCSI 6212.01C, Interoperability and Supportability of Information Technology and National Security Systems.*

(3) Interoperability, Compatibility, and Supportability Analysis. Planners identify interoperability, compatibility, and supportability requirements and assess them against documented capabilities. When the mission permits, key interoperability and compatibility solutions will be validated before mission execution. Any shortfalls or deficiencies are assessed for operational and mission impact. In cases where operational and mission impact are too severe, the communications system planners determine whether it is operationally and technically feasible to resolve the problem in theater; if not, they request assistance from higher HQ.

(4) Capability Analysis. Based on mission analysis, information needs, interoperability, compatibility, and supportability analysis, communications system planners identify the C2 systems and networks that can support the OPLAN. Service component planners should be brought into capabilities analysis as soon as possible. Capabilities analysis is a daily assessment during all phases of the operation. In the joint environment, attention is given to the organic C2 systems and networking capability of deploying and in place units. Provisions must also be made for higher HQ connectivity to its subordinate HQ and component-to-component connectivity. Normally, a Service component unit is assigned responsibility for communications system support at each HQ or other element, and a standard package of C2 systems and networks is provided. The standard packages are matched against operational needs. Listings of overages and shortages are produced for each location, major platform, and mission. Special attention is given to the time-phased force and deployment data (TPFDD)

(5) Allocation of Communications System Assets. After the template is developed, joint force and Service and functional component planners must examine all available resources and plan a tailored communications system. III-15

Interoperability is one of the many factors that must be considered in the communication plan and should be achieved primarily by a commonality of equipment, software, and systems. Planners must know the capabilities and limitations of the other component communications system resources

and must be able to integrate them into the joint communications system plan. The joint communications-electronics operating instructions (CEOI) and communications security must be coordinated with Service CEOI/signal operating instructions and communications security must also be coordinated .III-19

C. CHAIRMAN OF THE JOINT CHIEF OF STAFF INSTRUCTIONS

The Chairman of the Joint Chief of Staff Instructions (CJCSI) provides policy and guidance that does not involve the employment of forces. The instruction is of indefinite duration and is applicable to external agencies or both the Joint Staff and external agencies. It remains in effect until superseded, rescinded, or otherwise canceled. CJCS Instructions, unlike joint publications, will not contain joint doctrine and/or joint tactics, techniques, and procedures (<http://usmilitary.about.com/od/glossarytermc/g/cjcsi.htm>). The following instructions were selected for this thesis based on the I² significance to the Armed Forces.

1. CJCSI 3100.01A September 1, 1999, Directive Current as of September 12, 2003

JOINT STRATEGIC PLANNING SYSTEM

This instruction provides joint policy and guidance on, and describes the responsibilities and functions of, the Joint Strategic Planning Systems (JSPS). The Chairman of the Joint Chiefs of Staff (JCS) utilizes this flexible system with the intent to interact with other DoD systems by providing support through military advice to the DoD Planning, Programming, and Budgeting Systems (PPBS), and strategic guidance to the Joint Operation Planning and Execution System (JOPES) (Enclosure A, Introduction, 1., A-1.) The utilization of JSPS provides a structured integrative plan that formulates strategic and contingency plans which shape requirements and assessment of capabilities. The Chairman of the Joint Chiefs of Staff provides this comprehensive strategic information regarding the Armed Forces to the President and Secretary of Defense.

2. CJCSI 6212.01D March 8, 2006, Directive Current as of March 14, 2007

INTEROPERABILITY AND SUPPORTABILITY OF INFORMATION TECHNOLOGY AND NATIONAL SECURITY SYSTEMS

This set of instructions establishes policies and procedures for developing, coordinating, reviewing, and approving Information Technology (IT) and National Security System (NSS) Interoperability and Supportability (I&S) needs across the Armed Forces. The intent is to ensure that DoD components 1) meet operational needs of US forces; 2) are interoperable with existing and proposed IT and NSS; 3) support the existing and planned global information grid; 4) interoperate with allies and coalition partners; 5) be net-ready; and 6) enable US forces to protect, detect, restore and respond to essential information systems security situations. P. 3 of CJCSI 6212

This instruction drove the establishment the Joint Interoperability Certification Test Command (JITC). Many within the acquisition community work with JITC to ensure standard interface requirements related to a program are verified via the conduct JITC standards testing prior to fielding. JITC follows the processes outlined in Chairman, Joint Chiefs of Staff Instruction 6212.01, *Interoperability and Supportability of Information Technology and National Security Systems*, to perform their joint interoperability test and certification mission related to approving IT and NSS interoperability. JITC also establishes procedures for performing interoperability test certification using a new “Net-Ready” approach, which is a central network that focuses on the contributions and consumption of information within an organization.

As the GIG evolves toward a net-centric architecture, interoperability testing must also evolve. Increasingly, the requirement will be to test a system’s ability to successfully discover and employ the appropriate information resources within the context of the GIG. Of course, real-world capability development and testing are rarely simple, and the DoD has provided several mechanisms for identifying and seeking solutions to current or foreseen interoperability problems. DoD policy clearly states that all IT and NSS, regardless of Acquisition Category (ACAT), must be tested and certified for interoperability before fielding.

D. DOD INSTRUCTION 4630.8, PROCEDURE FOR INTEROPERABILITY AND SUPPORTABILITY OF INFORMATION TECHNOLOGY (IT) AND NATIONAL SECURITY SYSTEMS (NSS)

According to the DoD Instruction 4630.8, 2004, three implementations are to be set forth support IT and NSS: 1) an updated policy and responsibilities for

interoperability and supportability, 2) a capability-focused approach for IT and NSS ensuring life-cycle interoperability throughout the DoD, and 3) a Net-Ready Key Performance Parameter to assess net-ready attributes for technical and end-to-end operational effectiveness.

LIST OF REFERENCES

- Agnes, M. (Ed.). (2006). Webster's New World College Dictionary (4th ed.). Cleveland, OH: Wiley.
- Alsene, E. (1994). Computerized Integration and the Organization of Work in Enterprises. *International Labour Review*. (133:5-6) 657-677.
- Anderson, M., B. Winterstine. (2003, February). *Gaps, deficiencies, and the C4ISR Solution*. Seapower. Retrieved August 12, 2008, from http://findarticles.com/p/articles/mi_qa3738/is_200302/ai_n9214211
- Army FCS Program Manager. (2008, April 24). Program Overview. Retrieved May 10, 2008, from <https://www.fcs.army.mil/program/index.html>
- Bassett, D. & Emery, D. (2005, September – October). SOSCOE-The Glue That Holds FCS Together. ARMY AL&T, 22-23.
- Bhuta, J., (2007, January 29). University of Southern California, COTS Interoperability. Retrieved April 24, 2008, from <http://sunset.usc.edu/csse/TECHRPTS/2006/usccse2006-608/usccse2006-608.pdf>
- Blanchard, B. & Fabrycky, W. (2006). *Systems Engineering and Analysis*. 4th ed. Upper Saddle River, NJ: Pearson Prentice Hall.
- Boeing. (2008). Space Shuttle Orbiter. Retrieved April 30, 2008, from <http://www.boeing.com/history/bna/shuttle.htm>
- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3100.01A; Joint Strategic Planning System; 1 September 1999; discusses Joint Vision 20xx in Enclosure B.
- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01D; Interoperability and Supportability of Information Technology and National Security Systems. (March 8, 2006).
- Congressional Research Service. (2008, June). *Coast Guard Deepwater Acquisition Programs: Background, Oversight Issues, and Options for Congress*. CRS Report for Congress. Retrieved August 2, 2008, from <http://www.fas.org/sgp/crs/weapons/RL33753.pdf>
- Department of Defense Instruction Number 4630.8 (2004). *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*. Washington, DC: Government Printing Office. Retrieved May 15, 2008, from <http://www.dtic.mil/whs/directives/corres/pdf/463008p.pdf>

- Department of Homeland Security. (2007, January). Office of Inspector General, *110'123' Maritime Patrol Boat Modernization Project*, OIG -07-27.
- Ditmeyer, S. (2005, June). Network-Centric Railroading Utilizing Intelligent Railroad Systems. Proceedings of the 10th International Command and Control Research and Technology Symposium "The Future of Command ... Control..." McLean, VA. Retrieved April 30, 2008 from http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/005.pdf
- DSB. (1996, May). Combat Identification, Office of the Under Secretary of Defense for Acquisition and Technology. Retrieved July 27, 2008 from, <http://www.acq.osd.mil/dsb/reports/combatidentification.pdf>
- Engebretson, J. (2007, May). Seeking Integration through Interoperability. *Integration Intelligence. SDM*, 37, 5; ABI/INFORM Global, 91.
- Evans, M., Abela, A., Beltz, T. (2002, April). Seven Characteristics of Dysfunctional Software Projects. *CrossTalk, The Journal of Defense Software Engineering*. Retrieved July 6, 2008, from <http://www.stsc.hill.af.mil/crosstalk/2002/04/evans.html>
- Federation of American Scientists. (2000, May 17). Future Combat Systems. Retrieved May 4, 2008, from <http://www.fas.org/man/dod-101/sys/land/fcs.htm>
- Hartley, D. (2005) Successful Design, Development, and Integration of UA System of systems: Initial Findings from the Commonality Pathfinder Project. Retrieved April 28, 2008, from <http://home.comcast.net/~dshartley3/FCS/solution.htm>
- Hobday, M., Davies, A., Prencipe, A. (2005). Systems integration: a core capability of the modern corporation. *Industrial and Corporate Change*, 14(6), 1109-1143. Retrieved January 31, 2008, from ABI/INFORM Global database. (Document ID: 950902661).
- HQMC. (2004). Warfighting Concepts, Emerging & Enabling Capabilities. Distribute Common Ground/Surface System-Marine Corps (DCGS-MC). Retrieved May 5, 2008, from <http://hqinet001.hqmc.usmc.mil/p&r/concepts/2004/PDF/new%20CP04%20CHAP%202.pdf>
- Joint Publication 1 – Doctrine for the Armed Forces of the United States. (May 4, 2007).
- Joint Publication 6-0 – Joint Communications System. (March 20, 2006).
- Kablenet. (May 2007). MPs criticize combat ID systems. *The Register*. Retrieved June 18, 2008, from http://www.theregister.co.uk/2007/05/01/it_shortcomings_endanger_troops/

- Kaplan, J. (2006, June). *A New Conceptual Framework for Net-Centric, Enterprise-Wide, System-of-Systems Engineering* (v). Washington, DC: Center for Technology and National Security Policy, National Defense University.
- Knight, R. (2006, September). The University of Delaware Library. Statutory Law: A Research Guide. Retrieved April 25, 2008, from <http://www2.lib.udel.edu/subj/godc/resguide/statutor.htm>
- Langford, G., Franck, R., Huynh, T., Lewis, I. (December 14, 2007). *Gap Analysis: Rethinking the Conceptual Foundations*. Naval Postgraduate School Acquisition Research Sponsored Report Series (NPS-AM-07-051). Monterey, CA: Naval Postgraduate School.
- Luftwaffe Resource Center. Fi-103/V-1 Buzz Bomb.(n.d.). Retrieved June 24, 2008, from <http://www.warbirdsresourcegroup.org/LRG/v1.html>
- Maier, M., & Rechtin, E. (2000). *The Art of Systems Architecting*. New York: CRC Press.
- MIT. (2005). MITOPEN COURSEWARE. 16.885J/ESD.35J Aircraft Systems Engineering. Retrieved April 29, 2008 from www.ocw.mit.edu/OcwWeb/Aeronautics-and-Astronautics/16-885JFall-2005/CourseHome
- Morris, J. (2006). Aerospace Daily & Defense Report. Raytheon Reports 25 Orders For DCGS Integration Backbone. Retrieved April 28, 2008, from http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=aerospacedaily&id=news/BACK05096.xml
- National Research Council. (2007). *Human-System Integration in the System Development Process: A New Look*. Washington, DC: The National Academies Press.
- National Review. (1985, September). Horror Stories. Retrieved April 28, 2008, from http://findarticles.com/p/articles/mi_m1282/is_v37/ai_3926890
- NETWORK WORLD. (2008). Unmanned aircraft pose myriad problems to US airspace, GAO reports. Retrieved July 22, 2008, from <http://www.networkworld.com/community/node/27876>
- Parmley, J. (2006). University of Delaware. Expert: Failure leads to successful design. Retrieved May 3, 2008, from http://www.ce.udel.edu/Kerr_Lecture/Petroski%20Story%20UD.htm
- Peck, M. (2003, August). Desert Setting Tough on Combat ID Systems. *National Defense*. Retrieved June 18, 2008, from National Defense. http://www.nationaldefensemagazine.org/archive/2003/August/Pages/Desert_Setting3798.aspx

- Pei, R.S. (2000). *System-of-Systems Integration (System of systems) – A Smart Way of Acquiring Army C4I2WS Systems*, Proceedings of the Summer Computer Simulation Conference, 574-579.
- Pike, J. (2005). Intelligence. Distributed Common Ground Systems (DCGS). Retrieved April 30, 2008, from <http://www.globalsecurity.org/intell/systems/dcgs.htm>
- Public Law 104-106 104th Congress, A. (February 10, 1996).
- Public Law 105-261 105th Congress. (October 17, 1998).
- Public Law 107-314, 107th Congress. (December 2, 2002).
- Rifley, R. (2008, January 16). Personal communication. Robert provided background via presentation at System Integration workshop.
- Robbins, S. (2002). The Evolution of the Learning Content Management System. Retrieved July 25, 2008 from <http://www.learningcircuits.org/2002/apr2002/robbins.html>
- Rogers, M. (2003, October). Statement of Brigadier General Marc Rogers, USAF Director, Joint Requirements and Integration Directorate, J8, United States Joint Forces Command. Before the 108th Congress House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats, and Terrorism. Retrieved July 20, 2008, from <http://www.iwar.org.uk/rma/resources/c4i-interoperability/03-10-21-rogers.htm>
- SAFECOM, System of Systems Brochure. Retrieved July 19, 2008, from [http://www.safecomprogram.gov/NR/rdonlyres/FD22B528-18B7-4CB1-AF49-F9626C608290/0/SYSTEM OF SYSTEMSApproachforInteroperableCommunications_02.pdf](http://www.safecomprogram.gov/NR/rdonlyres/FD22B528-18B7-4CB1-AF49-F9626C608290/0/SYSTEM%20OF%20SYSTEMSApproachforInteroperableCommunications_02.pdf)
- Singletary, L. (2002). Empirical Study of Stakeholders' Perceived Benefits of Integration Attributes for Enterprise IT Applications. Eight Americas Conference on Information Systems, 2573-2579.
- Smith, D., Carney, D., & Morris, E. (2005, May). Interoperability Issues for Autonomic Computing. DEAS Workshop. Carnegie Mellon University, Software Engineering Institute. Sponsored report series.
- Talbot, David. (November 2004). How Tech Failed in Iraq. *Technology Review*, 107, 9, 36-44.
- Turso, J., Ainsworth, W., Dusang, L., Miller, D. and L., Smith. (2007, May). *U.S.S. Makin Island: Simulation-Based Analysis and its Role in Electric-Plant Control System Design*. Electric Ship Technology Symposium, Alexandria, VA.

- United States Department of Transportation. (March 2002). Federal Railroad Administration, Five-Year Strategic Plan for Railroad Research, Development, and Demonstrations. Washington, DC.
- United States Government Accountability Office. (February 1987). *Radio Frequencies – Earlier Coordination Could Improve System Use and Save Cost*. (GAO-87-42). Washington, DC: Government Printing Office. Retrieved July 18, 2008, from <http://archive.gao.gov/d2t4/132122.pdf>
- United States Government Accountability Office. (May 2001). *New Procedures Could Help Reduce Interference Problems*. (GAO-01-604). Washington, DC: Government Printing Office. Retrieved July 18, 2008, from <http://www.gao.gov/new.items/d01604.pdf>
- United States Government Accountability Office. (August 2003). *Issues Facing the Army's Future Combat Systems Program* (GAO-03-1010R). Washington, DC: Government Printing Office. Retrieved May 10, 2008, from <http://www.fas.org/man/dod-101/sys/land/gao031010.pdf>
- United States Government Accountability Office. (2003, March). *Steps Needed to Ensure Interoperability of Systems That Process Intelligence Data* (GAO-03-329). Washington, DC: Government Printing Office. Retrieved April 28, 2008, from <http://www.gao.gov/new.items/d03329.pdf>
- United States Government Accountability Office. (March 2004). *Coast Guard's Deepwater Program Needs Increased Attention to Management and Contractor Oversight*. (GAO-04-380). Washington, DC: Government Printing Office. Retrieved July 18, 2008, from <http://www.gao.gov/new.items/d04380.pdf>
- United States Government Accountability Office. (March 2005). *Future Combat Systems Challenges and Prospects for Success* (GAO-05-442T). Washington, DC: Government Printing Office. Retrieved August 11, 2008, from <http://www.gao.gov/new.items/d05442t.pdf>
- United States Government Accountability Office. (November 2005). *DOD Acquisition Outcomes, A Case for Change* (GAO-06-257T). Washington, DC: Government Printing Office. Retrieved April 28, 2008, from <http://www.gao.gov/new.items/d06257t.pdf>
- USA Today. (August 2006). Safety a concern as drones catch on. Retrieved July 14, 2008, from http://www.usatoday.com/tech/news/surveillance/2006-08-06-drones_x.htm?csp=34
- Valerdi, R. Ross, A, Rhodes, D. (October 2007). A Framework for Evolving System of Systems Engineering. Retrieved January 20, 2008, from <http://www.stsc.hill.af.mil/crosstalk/2007/10/0710ValerdiRossRhodes.html>

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Dr. John Osmundson
Naval Postgraduate School
Monterey, California
4. LtCol Scott Bey
United States Marine Corps
MARCORSYSCOM
Quantico, Virginia
5. Henry Cook
Northrop Grumman Ship Systems
Pascagoula, Mississippi
6. Robert Rifley
Northrop Grumman Ship Systems
Pascagoula, Mississippi